FAULT TREE ANALYSIS OF CANDU SHUTDOWN SYSTEM

By

DEVA DATTA SHARMA

NUCLEAR ENGINEERING AND TECHNOLOGY PROGRAMME

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

AUGUST, 1979

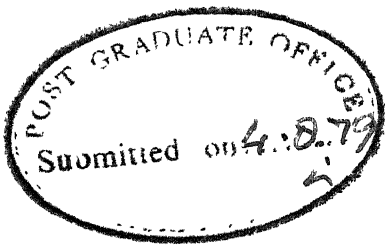
FAULT TREE ANALYSIS OF CANDU SHUTDOWN SYSTEM

A Thesis Submitted
In Partial Fulfilment of the Requirements
for the Degree of
MASTER OF TECHNOLOGY

By

DEVA DATTA SHARMA

to the
NUCLEAR ENGINEERING AND TECHNOLOGY PROGRAMME
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR
AUGUST 1979



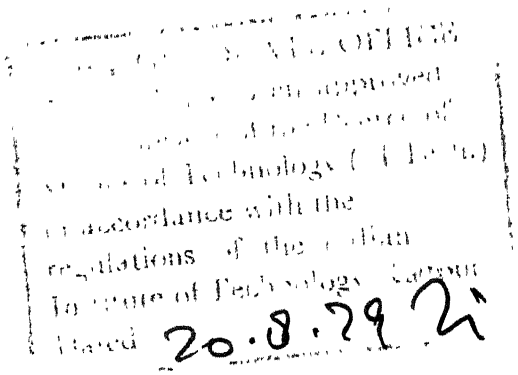
CERTIFICATE

This is to certify that the work presented in this thesis entitled, 'Fault Tree Analysis of CANDU Shut-Down System', has been carried out under my supervision and has not been submitted elsewhere for the award of degree.

K. Sri Ram

(K. Sri Ram)
Professor and Head
Nuclear Engg. and Technology Prog
Indian Institute of Technology,
Kanpur 208016

August, 1979



ACKNOWLEDGEMENTS

The profound indebtedness of the author towards his guide Prof. K. Sri Ram is inexpressible. Under his unerring guidance and enlightened discussions many a complicated problems turned out to be rather simple. His unfathomable patience and continuous encouragement always inspired me during this work. I have greatly enjoyed his company both as a supervisor and as a friend.

The requisite information on CANDU Shut-down System was provided by Mr. P. Arumugham, General Manager, Quality Assurance Group, BHEL and Mr. A. Bhoomiaha of PPED. This invaluable help is gratefully acknowledged.

The author had many fruitful discussion sessions with Vishnu and Romil in preparing mathematical models of shutdown system. Rakesh, Harish and Pradeep assisted in obtaining the volumes of indispensable WASH-1400. Deepak has helped immensely in literature survey. Author wishes to express his sincere thanks for all of them.

Mr. J.K. Misra has done a commendable typing job. Buddhi Ram and Ayodhya Prasad have been very cooperative with cyclostyling work.

Deva Datta Sharma

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

Notations

α	:	Weibull distribution scale parameter
β	:	Failure rate, /hr.
σ	:	Standard deviation
μ	:	Mean
h	:	hazard function
q,Q	:	unavailability
Eij	:	Event ij
P,Pr	:	Probability
R	:	Reliability
T	:	Top event

Subscripts:

CM	:	Common mode failure
IC	:	Instrument channel
LP	:	Liquid poison
R	:	Shutdown rod
T	:	Top event

Abbreviation:

CANDU	:	Canadian Uranium Deuterium Reactor
EMSR	:	Electromechanical Shutdown rod
ESF	:	Engineered Safety Features
GHT	:	Gas Header Tank
LHT	:	Liquid Header Tank
LPR	:	Liquid poison rod
NPP	:	Nuclear Power Plant

ABSTRACT

Reactor shutdown system is the most critical component amongst engineered safety features of a nuclear reactor. Its reliability estimation is rendered difficult because of the lack of failure data and the complexity of the system. Fault tree analysis is an adequate technique for the unavailability estimation of such systems. Fault Trees express the system failure as boolean function of the failure of basic components of the system. Failure data is usually available for basic components and can be used for point and confidence interval estimate of system of unavailability. To propogate the uncertainity in basic component failure data Monte-Carlo simulation can also be used.

CANDU shutdown system comprises of Electro-mechanical shutdown rods and Liquid poison injection each of which includes sensors, instrument channels, mechanical and fluidic subsystems. Published work so far have analysed sensors and instrument channels, for PWR's (i.e. only electro-mechanical shutdown rods), and have reported a value of $\sim 10^{-5}$ for the unavailability of the reactor protection system. The basic component failure rate is assumed to be constant and to have a lognormal distribution.

Present work analyses the entire CANDU shutdown system. Mathematical models are developed to analyse time constrained behaviour of the shutdown system. The affect of aging of basic components is also analysed. Instead of using lognormal distribution for the failure rate of all basic components, Weibull distribution is used because the later has lower standard deviation. From the analysis in present work an unavailability of $\sim 10^{-4}$ is obtained. It has been concluded that time constraint on system operation and the aging of components over a period of a year does not significantly affect the system unavailability.

CHAPTER I

INTRODUCTION

Although Nuclear Power Plants have demonstrated definite advantages over conventional power plants in environmental, ecological and economics aspects, their existence and efforts to pursue expansion are challenged, rightly, on the grounds of serious potential hazards posed by their presence in an eventual accident. Therefore, safe operation of reactor is of utmost concern to the design engineers, operations people and the public at large.

1.1 CONCEPT OF RISK:

A reactor is said to operate safely if under all conceivable and realistic accidents the risk to the society is acceptable. While making the preceding statement we are immediately confronted by two problems, first, what is the acceptable risk limit to the society and second how can we quantify this risk? No definite solution can be given for the first problem because the parameter involved, risk, as conceived by the society depends upon several factors such as time, nature of society, external circumstances of the society, the degree of technological progress and affluence etc., therefore the best one can do is to compare the risks

posed by a new technology with the risk posed by an already accepted technology. Risk as defined by dictionary means, 'possibility of loss or injury to a person and property'. To restrict the vagueness of the term in reactor safety study'risk' encompasses potential fatalities and injuries to people and property . In order to quantify societal risks from accidents following definition is used [1].

$$\text{RISK}\left\{\frac{\text{Consequence}}{\text{time}}\right\} = \text{Frequency}\left\{\frac{\text{Events}}{\text{Unit time}}\right\} \times \text{Magnitude}\left\{\frac{\text{Consequences}}{\text{Event}}\right\}$$

Another definition usually encountered and preferable when dealing with low frequency events is [2 , 3],

$$\text{RISK} = \left\{\begin{matrix}\text{Probability of occurance}\\ \text{of event}\end{matrix}\right\} \times \left\{\begin{matrix}\text{Consequence}\\ \text{per event}\end{matrix}\right\}$$

It is easy to observe that both the definitions express the same information on different scale.

Risk determination, therefore, requires estimation of the two terms viz., consequence per event and the probability of the event. An accident leads to multifacet consequences and representing all of them in a common unit is not always possible. The consequences usually include fatalities and injuries to people and damage to property. In some studies consequence of occupational fatalities and non-fatal injuries are expressed as lost man-hours whereas in other studies consequences are converted into monetary penalties

however, such an approach suffers the disadvantage of lacking an universally acceptable criterion for conversion of consequences into equivalent man-hours or monetary value. In order to circumvent such difficulties inseparable from the concept of a common unit, reactor safety studies [1] give up such an attempt and have selected four types of consequences. These are:

a. Early fatalities,

b. Early illness,

c. Late health effects attributable to the accident,

d. Property damage.

Estimation of the probability of occurrence of an accident (an event) should incorporate interaction of accident prevention systems, systems safeguards and accident generating events. The most convenient approach would be to collect reactor accident data and using standard parametric estimation and statistical inference techniques to draw conclusions regarding a location parameter (mean, median or mode) and variance or confidence limits. For inferences drawn to be meaningful data should be adequate to permit conventional statistical analysis. Unfortunately, advanced engineering systems due to inherent high reliability, seriously lack accident data thereby defying conventional analysis. Moreover, because of the huge investment involved it is desirable to have an estimate of the probability of an accident before deciding over the final design, and this being the case

where no data is available on the system performance. Therefore, in either case, quantitative risk assessment requires use of analytical methods. Event trees and fault trees are such analytical methods.

1.2 RISK ASSESSMENT METHODOLOGY:

A Nuclear Power Plant is a technologically advanced and complex system. The operating experience to the date and acturial accident data available is highly deficient due to high reliability of the system. It is therefore not surprising that Event Tree and Fault Tree Methodology have become a very popular technique of risk assessment. Any accident in NPP system that can potentially lead to radioactivity release is included in overall risk assessment. The methodology employed, therefore, should be able to identify in principle the accidents that can lead to significant releases and determine their probability. Because of the potential hazard of such accidents many safety features are engineered into the system to check the propagation of accident and limit the consequences. Therefore, radioactivity release is preceded by an accident sequence involving the initiating event and unreliable operation of some of the engineered safety features (ESF). Obviously, for a given initiating event there may be more than one accident sequences that can lead to radioactivity release. Two different problems to be resolved at this stage are, first, how to identify an

initiating event that will lead to significant releases and second given an initiating event how does one identify all accident sequences. The logic for selecting an initiating event has been dealt with in ref. [4]. To identify the accident sequences Event Trees are used.

1.2.1 EVENT TREES:

An event tree is a logic method for identifying the various possible outcomes of a given event called initiating event [1]. In reactor safety analysis initiating event is a system failure. The total number of outcomes depend upon number of options available or engineered safety features built in to mitigate the consequence of the accident. For example, Fig. 1.1, depicts an event tree for reactor coolant pipe break. Subsequent to the initiating event 'pipe break' depending upon the performance of the options in headings B, C, D and E several accident sequences are obtained. In particular if there are N headings or options including the initiating event the number of resulting accident sequences will be 2^N-1. Usually N may be as large as 10 and it can be easily appreciated what a momentous task it would be to comprehend and analyse all of them. Fortunately, all accident sequences are not important and many of them can be dropped because they are [1],

a. meaningless

b. illogical

c. redundant

d. a preceding option whose failure will definitely complete the accident sequence no matter how the following options behave, has failed.

The last point (d) calls in the study of functional interrelationships such as [4],

a) Time dependent performance requirements for the physical systems needed to perform the various ESF (options) functions,

b) Failure of one function eliminates need for another.

c) Failure of one function leads to such physical processes that cause other functions to fail.

d) Effect of accident characteristics (as pipe break size) and location on the event tree and on the operability requirements for the systems providing ECC.

Based on such considerations an event tree can be reduced to convenient size as shown in Fig. (1.1).

1.2.2 FAULT TREES:

Event trees define failure of various options or ESF and risk assessment requires probability of failure of these systems. This task is performed by Fault Trees. Fault Tree analysis was introduced by Bell Telephone Laboratories in 1961 for performing safety evaluations of launch control

systems for Minuteman Program [5]. At 1965 Safety Symposium, sponsored by the University of Washington and the Boeing Co., several papers were presented that expounded the virtues of fault tree analysis [3]. The presentation of these papers marked the beginning of a widespread interest in the possibility of using fault tree analysis as a reliability estimation tool in the nuclear reactor industry. In the early 1970's great strides were made in the solution of fault trees to obtain complete reliability information about relatively complex systems [6 , 7 , 8]. The year 1975 witnessed the publication of the monumental task, 'Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants - WASH 1400', in which event tree and fault tree methodology has been applied for risk assessment of an entire NPP system. Since the publication of this work Fault Tree Methodology has gained extreme popularity and it is now very usual to come accross research papers on various aspects of Fault Trees in reputed journals on Reliability. More recently significantly growing interest was witnessed at 'The Symposium of Nuclear Systems Reliability Engineering and Risk Assessment' [9].

Fault Tree method reconstructs the undesired fault from the failure of basic components of the system through binary logic. In principle Fault Tree construction is relatively a simple exercise. Essential steps involved in Fault Tree construction are:

(i) A thorough understanding of the system to be analysed is a prerequisite. Fault trees assist in organising the knowledge of system but do not replace it.

(ii) Definition of TOP event. TOP event is the one whose probability of occurance is desired. The definition has to be precise and in terms of system hardware.

(iii) Now we look for events that can cause TOP event either together, or individually, or in some mixed mode. Their relation to TOP event is defined by boolean operators AND and OR and is conveniently represented by logic gates AND and OR.

(iv) These events are now individually treated as TOP events and step (iii) is repeated till we do not reach the events defining failures of such components whose data is available.

(v) Fault Trees for components which can fail in more than one mode are separately constructed and substituted at appropriate position in the systems fault tree.

(vi) Editing of the fault tree so constructed is done to avoid omissions, logical discrepancies and repetitions.

For a simple system Fault Tree construction can be done manually, however, while tackling complex systems there are many pitfalls. The worst pitfalls that confront one unskilled in performing Fault Tree analysis are over-sight and omissions. Significant omissions sometimes occur if the

analyst jumps two or more logical levels in his development of a deductive chain of factors and causes. For example, he may skip from initiation of a command to its acceptance, and neglect transmission. This tendency is minimized if one follows the rule of listing very direct immediate causes of any factor considered, before going on to consider the next lower level of causes[10]. Another problem with manual construction is that it is time consuming. The manual construction of all the fault trees reported in WASH-1400 would have taken for a skilled person 25 man-years of continuous work [11]. Because of these constructional difficulties automated fault tree construction methods have been developed.

The next step in fault tree analysis is the quantification of fault tree. Since the TOP event is related to basic component failure through binary logic, boolean algebra can be used to relate them, conversion of which to a probability expression is a simple step. Knowing unavailability of basic components to obtain point estimate of TOP event occurrence probability is a simple matter. The real problem comes in propagating the statistical error in basic component failure-data so as to obtain confidence limits on the TOP event estimate. When fault tree is extremely simple one can attempt to compute variance of top event using standard expressions and then find confidence limits using Tchebycheff inequality [12]. In another approach used by WASH-1400,

Monte-Carlo simulation is used to propagate error ranges. When dealing with practical Fault Trees, in either case, one has to resort to digital computers.

Figure 1.2 [13] is a schematic presentation of the noteworthy codes produced in past 10 years for Fault Tree Analysis. Group 1 are the fault tree construction codes, while groups 2, 3 and 4 are the analysis codes. The analysis codes can be divided into two general types: those which directly produces numerical results shown in group 4, and two step codes which first qualitatively (group 2), and then quantitatively (group 3) analyze the logic system.

The Fault Tree Construction code DRAFT [10] is based on synthetic Tree Model. Synthetic Tree Model is a synthesis method for constructing fault trees from small segments called component failure transfer functions. The component failure transfer functions are obtained from a system-independent analysis of every component appearing in the system for which the fault tree is to be constructed. Although DRAFT was written for certain electrical systems the technique is general enough to be used with nuclear industry.

Taylor's method [14] uses algebraic models for components with qualifiers to indicate which equations describe the operation or failure of the component. These qualified equations are then written for each component and the resulting collection forms the system model. This model

can then be applied to determine the consequences of any deviation in the input variables.

Tompkins and Powers [15] have suggested a method using input-output models for equipment. These models convey information regarding variable relationships when the components are working as well as the effects of components failures. Construction of the fault-tree begins with the identification of important deviations and it is through this search that the fault tree is built.

More recently Salem, Apostolakis and Okrent [3] have developed a computer-aided technique. The component behaviour is modelled using decision tables and the information thus obtained is used in fault tree construction.

Most of the Fault Tree quantification codes in groups 2 and 3 use Vesely's Kinetic Tree Theory [7] a methodology for obtaining time-dependent probabilistic results. The code PREP finds minimal cutsets of the system and these are required by the companion code KITT which computes the failure probabilities associated with the fault tree of the system. The code WAM/BAM like code SAMPLE of WASH-1400 probabilistically evaluates systems modelled with Boolean algebra. In another approach, Fussell and Vesely [15] use a matrix to organize increment results determined from a top-down (output-to-input) analysis of the logic. However, this essentially-searching routine does not use the matrices in the usual

matrix-mathematical sense. Semanderes [16] developed a FORTRAN computer program using Boolean algebra to calculate probabilities efficiently from logic expressions. He uses the unique factorization theorem of number theory (in which the product of prime numbers assigned to each of the input events retains the identification of these inputs) to keep track of product enteries. Schneeweiss [17] has recently presented a method to calculate probability from Boolean functions by algebraic techniques. Infact, methods based on Boolean expression minimization techniques such as algebraic, bit manipulation and Karnaugh graph have been proposed by various authors. Most recently Chamow [18] has proposed a technique based on graph theory.

Fault Tree Analysis is an all inclusive, versatile mathematical tool for analysing complex systems. Some of the advantages of the Fault tree analysis are [10];

(1) Directing the analyst to ferret out failures in a deductive way.

(2) Pointing out the aspects of the system important in respect to the failure of interest.

(3) Providing a graphical aid giving system management visibility to those removed from the system design changes.

(4) Providing options for qualitative or quantitative system reliability analysis.

(5) Allowing the analyst to concentrate on one particular system at a time.

(6) Providing the analyst with genuine insight into system behavior.

Fault tree models do have drawbacks. Most serious drawback is its inability to model failures that cannot be decomposed through binary logic, e.g., it cannot analyse the system's dynamics failure, such event are to be treated as primary event. Other disadvantages as has been discussed before include high cost, time consuming and possibility of existence of more than one fault trees if constructed manually.

Fig. (1.3) lists symbols and their definitions used in fault tree construction.

1.3 GENERAL DATA TREATMENT:

The quantification of fault tree can involve one of the two types of calculations: a point calculation, or a random variable evaluation. The point and random variable types of evaluation differ with regard to the goals and approaches which in turn depend upon the type of input data available. When the general goal is to derive a best estimate of a system parameter of interest, usually the system unavailability or failure probability the POINT VALUE calculation is used. Obviously, the input data available should be highly accurate to produce meaningful estimates. In practice extensive failure rate data to execute exact point estimation

is not available and feedback from field experience coupled with engineering judgement is used to determine applicability of data.

A more practical approach is to use the random variable technique. Because failure rate data is collected from several sources a range of values for failure rate is obtained which allows the data parameter to be treated as random variable to describe the probability associated with various possible values. This is the approach used in WASH-1400 [5] where to express uncertainity in failure rate data a lognormal distribution was fitted and the median as well as 5 and 95 percentile point values are tabulated. The lognormal distribution was chosen because of large variability in data, its flexibility, its consistency with reliability and data properties and because it is a standardly employed and straightforward distribution [5].

The large variability in the failure data of basic components is a serious drawback. Because this is a common problem in reliability estimation an attempt to include subjective information through the application of Bayes Equation has become a very popular technique. Bayesian reliability estimation methods have been applied to Nuclear industry systems [19,20]. Although Bayesian Method is a consistent way of incorporating subjective information, the

mathematical complexity in using it with a general distribution and results so far reported do not show that in practice it is superior to methods described before.

1.4 REACTOR SHUT-DOWN SYSTEM RELIABILITY ESTIMATION:

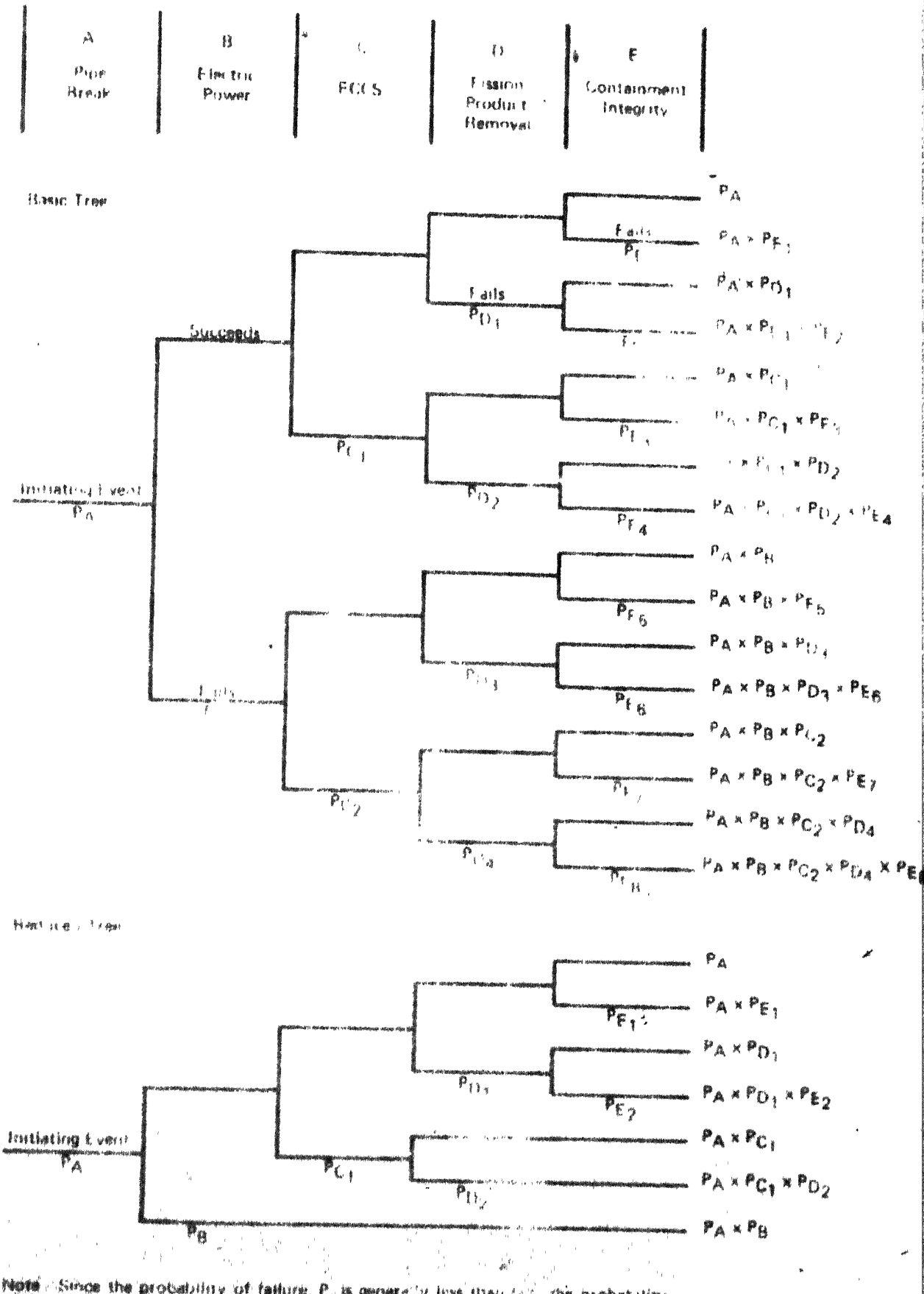
Reactor shut down system is the major reactor protection system and therefore its reliable operation is of utmost interest to reactor safety. WASH-1400 has restricted the analysis to instrumentation channels i.e. sensors, logic circuits and shut-down mechanism triggering circuits, omitting the mechanical and fluidis mechanisms for no obvious reason. Recently, Ullrich and Frich [21] have reported that for PWR's the main contribution to unavailability is from mechanical system and common mode failure. Table 5.1 tabulates the results obtained by WASH-1400 and Ullrich et al.[21].

1.5 PRESENT WORK:

Present work undertakes reliability estimation of reactor shut down system for a CANDU reactor, the type being proposed for NAPP. The shutdown system comprises of a principal shutdown mechanism, the Electro Mechanical Shut-down Rod and a back-up protection by Liquid Poison Rod mechanism. The successful operation of this system is time constrained, hence the present work includes into the analysis · the system unavailability due to chance failures, testing and maintenance, reliable operation subject to time constraints

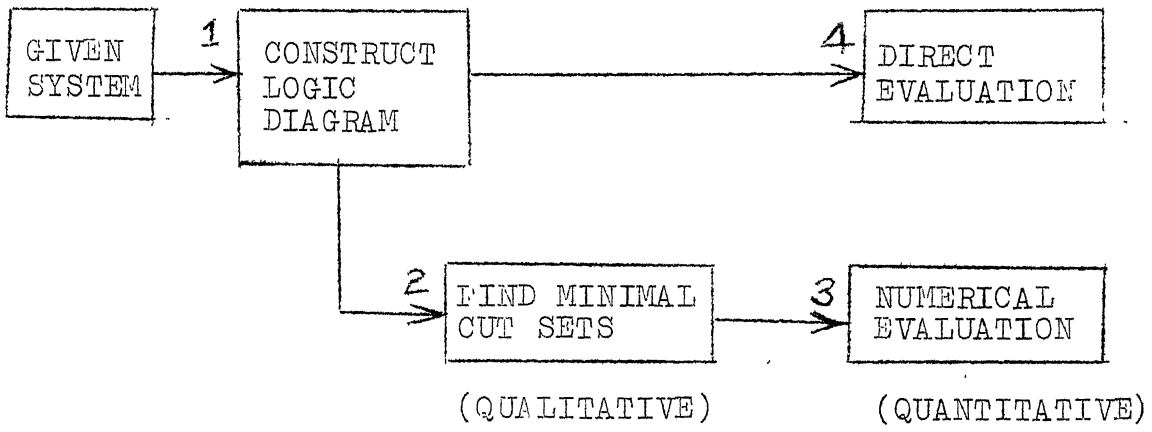
and deterioration in system performance due to aging, an aspect neglected in all previous works. The failure rate data is taken from [22] and [23] and treatment adopted in WASH-1400 [5] is followed. Distributions other than lognormal have been tried and the one having lowest variance is used. To propogate the error-range code SAMPLE [5] has been used with modification to include Weibull distribution along with already existing distributions.

The present work is presented in four chapters and three appendices. Chapter 2 contains description of the mechanism and operation of CANDU shutdown system, the unavailability expression for TOP event and the fault tree construction. Chapter 3 contains the computation of point estimate, confidence interval estimate of the TOP event unavailability and also the results of Monte-Carlo simulation for the time to trip for EMSR and LPR and for TOP event unavailability, assuming constant failure rate for basic components. In Chapter 4, effect of aging on component failure rate is considered and system unavailability is computed. Chapter 5 contains conclusions and an outline for the further work. Appendices A and B contain description of mathematical model of time to trip for EMSR and LPR respectively. Appendix C deals with data treatment procedure, basic probability expressions, treatment of testing and maintenance procedures and common mode failures.



Note : Since the probability of failure, P, is generally less than 0.1, the probability of success (1-P) is always close to 1. Thus, the probability associated with the upper (success) branches in the tree is assumed to be 1.

Fig. 1.1: Simplified Event Trees for a Large LOCA



TYPICAL PROGRAMS:

1) FAULT TREE CONSTRUCTION PROGRAMS

DRAFT (FUSSELL, 1973)
POWERS, TOMPKINS (1974)
CAT (1976)

2) MCS CODES: FIND MINIMAL CUT SETS
PREP (VESELY, 1970)
ELRAFT (SEMANDERES, 1971)

3) NUMERICAL EVALUATION CODES
KITT1, KITT2 (VESELEY, 1970)

MOCUS (FUSSELL, VESELEY, 1972)

TREEL

MICSUP (PANDE, ET AL. 1975)

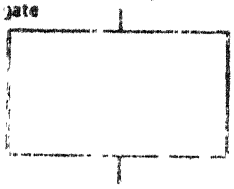
4) DIRECT EVALUATION CODES
SAMPLE (NUC.REG.COMM., WASH-1400, 1975)
WAM/BAM (RUMBLE, ET AL., 1975).

FIG. 1.2: Computer Codes for Fault Tree Analysis.

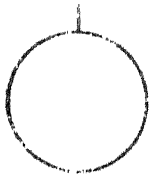
FAULT TREE SYMBOLISM

EVENT REPRESENTATIONS

The rectangle identifies an event that results from the combination of fault events through the input logic gate

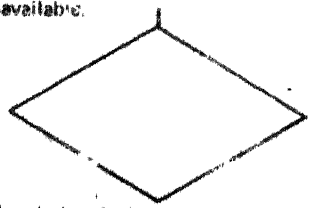


The circle describes a basic fault event that requires no further development. Frequency and mode of failure of items so identified are derived from empirical data

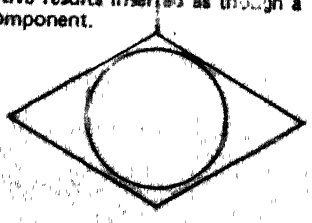


The triangles are used as transfer symbols. A line from the apex of the triangle indicates a transfer in and a line from the side or bottom denotes a transfer out

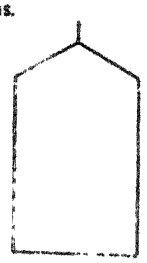
The diamond describes a fault event that is considered basic in a given fault tree. The possible causes of the event are not developed further because the event is of insufficient consequence or the necessary information is unavailable.



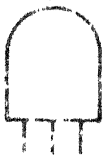
The circle within a diamond indicates a subtree exists, but that subtree was evaluated separately and the quantitative results inserted as though a component.



The house is used as a switch to include or eliminate parts of the fault tree as those parts may or may not apply to certain situations.



AND gate describes the logical operation whereby the coexistance of all input events is required to produce the output event



OR gate defines the situation whereby the output event will exist if one or more of the input events exists

INHIBIT gates describe a causal relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied. The conditional input defines a state of the system that permits the fault sequence to occur, and may be either normal to the system or result from failures.

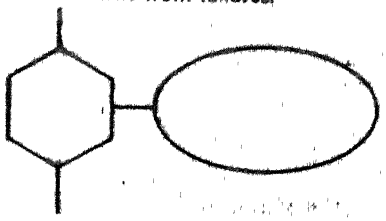


Fig. 1.3: Standard Fault Tree Symbols.

CHAPTER 2

FAULT TREE CONSTRUCTION

The reactor shut down system for CANDU reactor consists of a principle shutdown mechanism, the Electro-Mechanical shutdown Rod (EMSR) and a backup protection, the Liquid Poison Rod Shutdown (LPR). After an abnormality worthy of reactor shut-down is detected by monitoring instruments, the shutdown rod is expected to insert completely in the core in 2 seconds including time required to communicate failure through instrument channels. In case the shut-down rod fails to insert completely in 2 seconds it is considered to have failed and LPR is triggered. LPR is supposed to be filled in about 6 seconds (assumed for this study, could be anywhere from 2 seconds or higher) after being triggered failing which the Reactor Shut down System is considered to have failed.

2.1 ELECTRO MECHANICAL SHUTDOWN ROD SYSTEM:

To increase the reliability it is a standard practice to introduce redundancy into the system. Fig. 2.1 shows the simplified diagram of a EMSR and retains all the essential features of the original system [24,25]. Because of reactor physics consideration 12 such rods are required to introduce sufficient poison into the core in order to stop fission

chain reaction. Strictly speaking, it can be shown that even lesser number of rods will suffice [21], however, to increase the reliability 14 EMSR's are provided in the reactor. These 14 rods are triggered in pairs by 7 scram signal circuits.

The operation of a single EMSR is as follows. On receiving scram signal the rotating magnetic clutch MCP under the force of release springs SR is disengaged. Under the weight of shutdown rod the cable on the drum unwinds freely and is guided by pulleys P1 and P2 and the guide tube. The fall of rod is impeded by the friction between gears, between shafts and bearings and viscous drag due to the moderator. To overcome the effect of these impeding factors acceleration spring SPR 1 is provided. Under normal condition the rod is pulled against the SPR 1 so that on release very high initial velocity is achieved. At the end of journey the rod comes to rest on a support SP and to absorb vibrations a damping spring SPR2 is provided.

2.1.1 FAULT TREE FOR EMSR:

The EMSR system is said to operate successfully if 12 out of 14 rods reach the end support SP in guide tube within 2 seconds and rest on it. Because rods are triggered in pair by 7 scram signal circuits, failure of 2 or more instrument channel out of the 7 or failure of 3 out of 14 rods to insert completely in the core without damaging the support is considered as EMSR system failure. Therefore,

Failure of EMSR System = Failure of two or more of the instrument channels

OR

Failure in safe insertion of 3 or more out of 14 rods

Hence, using standard combinatorial algebra results,

Pr (Failure of EMSR System)

$$= 2-[\,(1-q_{IC})^{7} + 7q_{IC}(1-q_{IC})^{6} + 14\,q_{R}(1-q_{R})^{13} + 91q_{R}^{2}(1-q_{R})^{12}] \qquad (2.1)$$

where q_{IC} : Probability of failure of single instrument channel

q_{R} : Probability of failure of a single EMSR

As has been mentioned in Chapter 1, the determination of q_{IC} has been a favourite of most of the workers in this field and an attempt to determine q_{R} as defined here has not yet been undertaken. In the present study determination of q_{IC} is not repeated and its value is taken from WASH-1400. To find q_{R} fault tree analysis is undertaken for a single EMSR.

TOP event for the fault tree of EMSR is defined as:

'Failure of EMSR to fall to the bottom in 2 seconds and rest on the end support, SP'.

Following the fault-tree construction method suggested in Chapter 1, fault-tree for this case can be easily drawn and is shown in Fig. 3.1. For all basic events of fault-tree except RFF-2 (Rod fails to fall in 2 seconds) failure data is available in the literature [5, 23]. The data treatment is dealt with in Appendix C and the form in which they are used is tabulated there. Event RFF-2 lacks data and because of complex dynamic interrelationship between components further decomposition through binary logic is not possible. To resolve the problem of lack of data a mathematical model of EMSR has been developed, details of which are given in Appendix A. In brief, this model undertakes a realistic analysis of EMSR to produce time required to travel a specified distance under gravity and against the moment of inertia of rotating components, friction in bearings and between moving parts, buoancy due to moderator (D_2O) and viscous drag. The time dependent acceleration of rod is given by,

$$a(t) = \frac{W+wL_o-B_o+wl(t) - F(t)-B(t) - \sum \frac{I}{v} \theta^o \frac{d\theta^o}{dt}}{W + wL_o + w\, l(t)} g \qquad (2.2)$$

where,

W : weight of rod

w : weight of rope per unit length

L_o : length of unwound rope at $t = 0$

$l(t)$: length of rope unwound in time t

B_o : buoancy at time t = 0

B(t): buoancy plus viscous drag at time t minus B_o

I : moment of inertia of a rotating component

v : velocity of rope

θ^o : angular velocity of rotating component

g : acceleration due to gravity

F(t): sum of frictional forces between various components.

Equation (2.2) is a nonlinear, nonhomogeneous equation where nothing is known about a(t), v(t), l(t) except initial conditions and that they satisfy equation (2.2). This equation is solved by 'marching process'.

2.2 LIQUID POISON ROD SHUTDOWN SYSTEM:

Liquid poison rod shutoff system provides backup protection to the reactor shutdown. Fig. 2.2 shows flow-sheet of a LPR shut-off system. There are 14 such systems, 2 being redundant. The liquid shutoff rods are in the shape of U-tubes. One leg of this tube penetrates through the calandria and the other is outside the calandria. The main equipment in the system are pumps, helium compressors, storage tanks and valves. Each U-tube, connected between a gas header tank and a liquid poison header tank constitutes one liquid poison shut-off rod mechanism [25].

The liquid poison is held out of the core by means of a controlled differential pressure between gas and liquid

poison headers. When a scram signal is received the solenoid valve interconnecting liquid header tank (LHT) and Gas Header Tank (GHT) is deenergised resulting in equilisation of pressure in two tanks and as a result liquid poison is made to rise in the poison tubes. A shorter poison insertion time can be achieved by deenergizing another solenoid valve which is on the pipe line connecting LHT to Boaster cylinder.

2.2.1 FAULT TREE CONSTRUCTION:

The LPR shutoff system is said to operate successfully if 12 out of 14 rods are filled with liquid poison in about 6 second on failure of EMSR system. Therefore,

Failure of LPR System = (Failure to sense failure of EMSR system)
OR
(Failure to fill 12 out of 14 rods with liquid poison in about 6 seconds)

Hence,

$$\Pr(\text{Failure of LPR system}) = \Pr\{\text{13 out of 14 rods Fall to bottom in 2 seconds but one or more breaks through the support}\} + \Pr\{\text{Failure to fill 12 out of 14 rods with liquid poison in about 6 seconds}\}$$

$$= [1-14q_{RFF2}\,(1-q_{RRF2})^{13}].[1-q_{SB}^{13}] + [1-q_{LP}^{14} + 14q_{LP}\,(1-q_{LP})^{13} + {}^{14}C_2\,q_{LP}^2\,(1-q_{LP})^{12}] \quad (2.3)$$

where q_{RFF2} : Probability of failure to rod to fall in 2 seconds

q_{SB} : Probability that support does not break

q_{LP} : Probability of failure to fill a LPR in about 6 seconds

The probabilities q_{RFF2} and q_{SB} are obtained from the analysis of EMSR system. To find q_{LP} fault tree analysis is undertaken for a single LPR system.

TOP event for the fault-tree is defined as:

'Failure of Liquid Poison to fill the liquid rod in about 6 seconds.'

Fault Tree is shown in Fig. 3.2. For all basic events except event 1 failure data is available and the data treatment is given in Appendix C. Event 1 is of the same kind as RFF2 in previous article. Here too to resolve the problem of lack of data a mathematical model has been developed, details of which are given in Appendix B. In brief, this model computes the time required to fill a LPR. The He-gas flow circuit and the liquid flow circuits are considered as coupled circuits with unsteady flow. For liquid flow circuit neglecting thermodynamic changes in liquid properties, equation governing acceleration of rise of liquid in liquid rod is given by,

$$C_1(t)\,\frac{dV}{dt} + C_2(t)\,V^2 - C_3(t) = P_1(t) - P_2(t) \qquad (2.4)$$

where $V(t)$: velocity of liquid level in LPR

$P_1(t)$: He-pressure in LHT

$P_2(t)$: He-pressure in GHT

$C_1(t)$, $C_2(t)$, $C_3(t)$ are functions of liquid level at different sections along the liquid flow circuit.

The unsteady gas flow is considered to be steady state over a small time interval. A constant cross-sectional area pipe through which gas flow is adiabatic is being considered. The end pressures and Mach numbers are related by,

$$\frac{P_1}{P_2} = \frac{M_2}{M_1} \sqrt{\frac{1 + \frac{K-1}{2} M_2^2}{1 + \frac{K-1}{2} M_1^2}} \qquad (2.5)$$

where gas flow is from end 1 to 2, P_1, P_2 and M_1 are known and thereby M_2 can be calculated. Knowing M_2 the rate of inflow of gas (by mass balance), pressure and temperature changes can be computed, where suffix 1 and 2 denote conditions in tanks 1 and 2, flow is from tank 1 to 2, M is Mach number, P is pressure and K is the ratio of specific heats C_p/C_v for the gas.

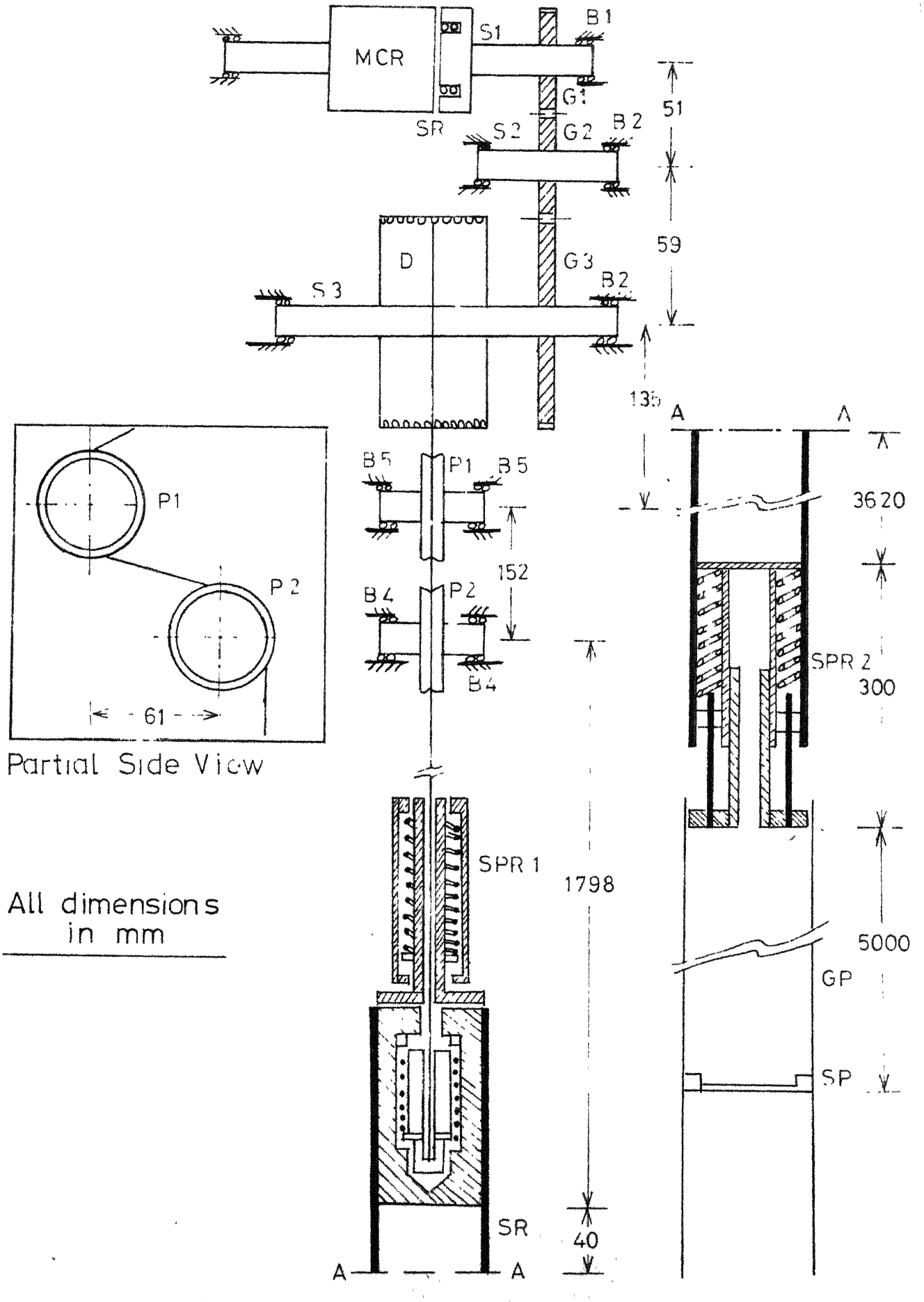


Fig. 2·1 Electro mechanical shut down rod

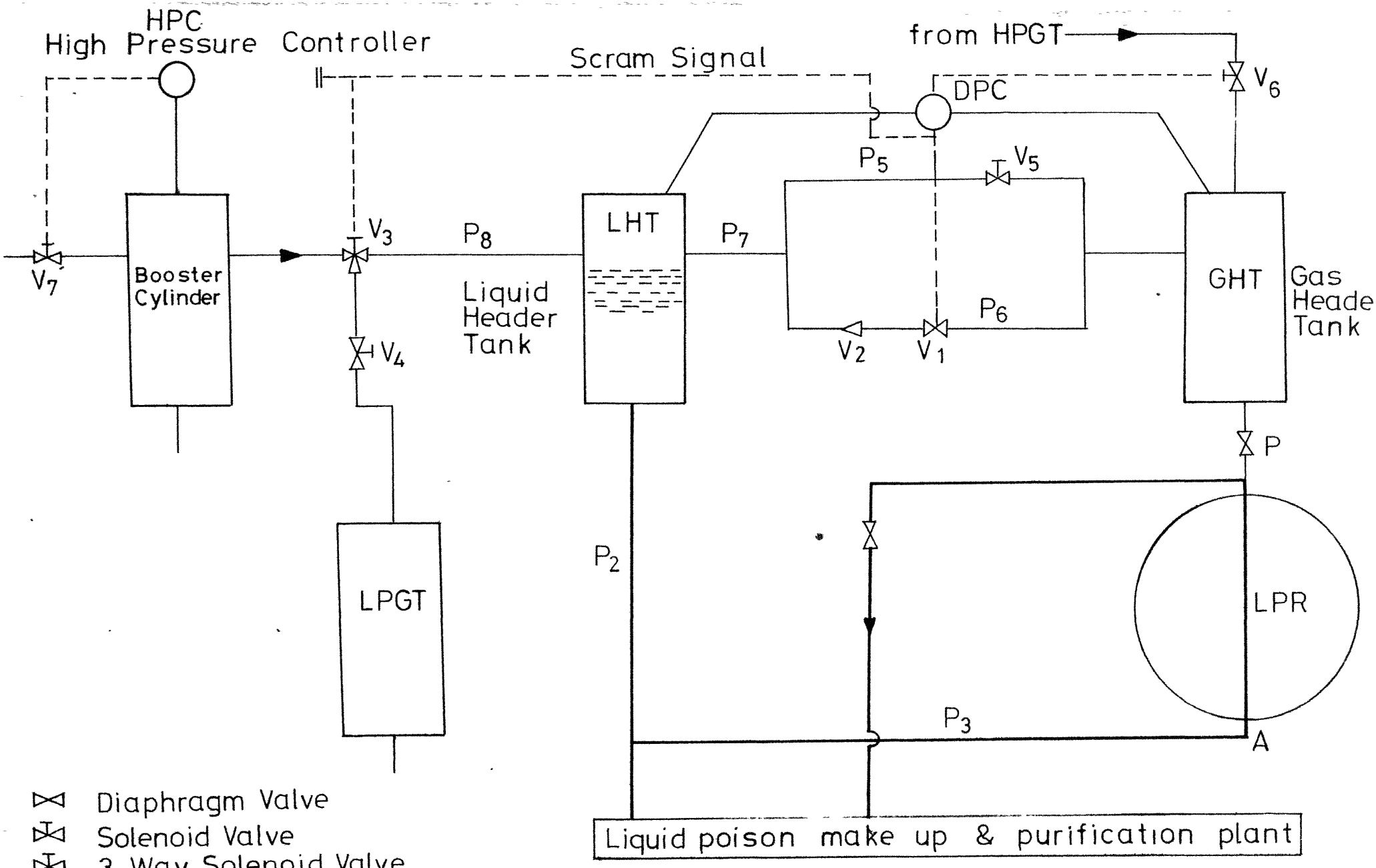


Fig. 2·2 Liquid poison shut off rod system

CHAPTER 3

FAULT TREE QUANTIFICATION

Appendix C discusses the computation of primary event probability or basic component unavailability over a given time from known chance failure rate. Considerations of repair and preventive maintenance are also discussed and used where applicable.

Given a fault tree the top event T can be expressed as boolean function of primary events E_i such as

$$T = f(E_1, E_2, E_3, \ldots, E_x) \tag{8.1}$$

For fault trees this can be written as

$$T = M_1 + M_2 + M_3 + \ldots + M_n \tag{3.2}$$

The events M_i are secondary events consisting of intersections of primary events,

$$M_i = \bigcap_{K=1}^{m} C_{i_k} \tag{3.3}$$

where no M_i is a subset of another M_j. With the expression in this form the M_i are termed the critical paths or minimal cut sets of the fault tree.

The probability of T for small probability events can be written as,

$$P(T) \simeq \sum_{i=1}^{n} P(M_i) \tag{3.4}$$

and if primary events are independent then,

$$P(M_i) = \sum_{k=1}^{m} P(C_{i_k}) \qquad (3.5)$$

In case, common mode failures exist, they are included and quantified as has been explained in Appendix C.

Given $P(C_{i_k})$ and the associated error factor the TOP event unavailability and error spread can be computed by one of the following methods:

a. When fault tree is simple statistical distribution algebra can be used to compute the location parameter and the variance of TOP event unavailability. Confidence limits can be derived by using Tchebeshev's inequality or by assuming a distribution for TOP event.

b. When Fault Tree is complicated it is convenient to use Monte-Carlo simulation of Fault Tree. Monte-Carlo simulation is expected to produce lower variance.

On reviewing the data available it can be seen that the standard deviation and location parameter are of the same order. In samples having such a high variance it is meaningless to talk of location parameter estimate with any consistency. Therefore, the relative superiority of the two methods does not depend so much upon their producing approximately equal location parameter estimate but upon producing lower variance in final result. In this chapter the results on the

probability of TOP event as computed by the two methods will be presented.

3.1 POINT AND INTERVAL ESTIMATION FOR TOP EVENT:

Given a fault tree we can, in principle, always compute mean (μ_T) and variance (σ^2) of the TOP event using standard results. This is more easily done when the fault trees are simple.

To compute 5 % and 95 % confidence bounds we use Tchebycheff inequality [12] given as

$$P\left[\,|T-\mu_T| \leq k\,\sigma_T\,\right] \geq 1 - \frac{1}{k^2} \tag{3.6}$$

The Tchebycheff inequality can be improved and written as [12],

$$Pr\,[T < d] \leq \frac{\sigma_T^2}{\sigma_T^2 + (\mu_T - d)^2}, \quad d \leq \mu_T \tag{3.7}$$

and

$$Pr\,[T < d] \geq 1 - \frac{\sigma_T^2}{\sigma_T^2 + (\mu_T - d)^2}, \quad d \geq \mu_T \tag{3.8}$$

Therefore 5 % confidence bound is given by,

$$L_{.05} = \mu_T - \sigma_T \sqrt{19} \tag{3.9}$$

and 95 % confidence bound is given by

$$U_{.05} = \mu_T + \sqrt{19}\ \sigma_T \tag{3.10}$$

Another method for computing confidence bounds is to select an approximate density function $f_T(t)$ for the TOP

event. Apostolakis and Lee [12] have used Johnson S_B distribution and have obtained results in good agreement with Monte-Carlo simulation results. The S_B distribution is given by

$$f_X(x) = \frac{1}{\sqrt{2\pi}\,\sigma_x\,(1-x)x} \exp\left[-\frac{\frac{1}{2}\{\ln[(1-x)/x]-\mu_X\}}{\sigma_X^2}\right] \qquad (3.11)$$

where α is TOP event probability.

For low probability events S_B distribution reduces to lognormal distribution and this explains the good agreement of results with Monte-Carlo simulation where lognormal distribution was fitted on the sample space simulated for the TOP event.

For a lognormal distribution with parameters μ and σ the 5 % bound is given by

$$L_{.05} = \exp(\mu - 1.6145\,\sigma) \qquad (3.12)$$

and 95 % bound is given by

$$U_{.05} = \exp(\mu + 1.6145\,\sigma) \qquad (3.13)$$

Another noteworthy distribution is Weibull. Experience stipulates that Weibull distribution can closely approximate mixtures of distribution and thereby adequately handle hetrogeneous population. The flexibility of Weibull distribution is a great asset. The density function of Weibull distribution is given by

$$f_X(x) = \frac{\beta}{\alpha} \left(\frac{x}{\alpha}\right)^{\beta-1} \exp\left[-\left(\frac{x}{\alpha}\right)^{\beta}\right] \qquad (3.14)$$

where α and β are parameters of Weibull distribution. β is shape parameter and α is location or scale parameter.

The 5 % confidence bound is given by

$$L_{.05} = \alpha\,(.0512932)^{1/\beta} \qquad (3.15)$$

and the 95 % confidence bound is given by

$$L_{.95} = \alpha\,(2.9957)^{1/\beta} \qquad (3.16)$$

3.2 MONTE CARLO SIMULATION [5]

When complexity of the fault tree forbids analytical treatment Monte Carlo simulation is used and is considered a very efficient method. Even in case of simple fault tree whose basic components can have a variety of unavailability density functions Monte-Carlo simulation offers an efficient and realistic treatment of data to generate failure data for TOP event.

Given a boolean function, $Y = f(X_1, X_2, \ldots, X_n)$, values of location and dispersion parameters of independent variables and associated density function the Monte-Carlo simulation consists in sampling $x_1, x_2, \ldots, x_n$ from input variable distributions and evaluating the function Y. This sampling is repeated N times and resultant sample space of Y are ordered

in ascending value $y_1 < y_2 < \cdots < y_n$ to obtain the limits of the distribution.

Monte Carlo simulation requires considerable computer time depending upon sampling size is N. To use the method efficiently failure-rate coupling technique is used in which only one sample is drawn for all similar, generic class of faults and common mode failures. The effectiveness of this modification is better appreciated while analysing large fault trees.

Computer code SAMPLE [5] is used for monte carlo simulation with modification to incorporate Weibull distribution.

3.3 FAULT TREE QUANTIFICATION FOR EMSR:

Fault tree in Fig. 3.1 is used to find TOP event unavailability by methods discussed in Sections 3.1 and 3.2. Common cause failures are identified and assuming a scheduled testing and maintenance every month, unavailability contributions due to common cause failures, testing and maintenance are included using techniques discussed in Appendix C. The data used for events E1 to E15 is taken from Appendix C and that for event E16 from Monte Carlo simulation of EMSR to produce time to fall to support SP. Results of Monte Carlo simulation of EMSR, data used, point estimation and Monte Carlo simulation of fault tree of EMSR are presented in Table 3.1 computation of point estimates and confidence bounds is given in Section (3.3.1).

3.3.1 COMPUTATION OF POINT ESTIMATES OF THE UNAVAILABILITY OF A SINGLE EMSR:

Fault Exposure Time = 720 hrs. (1 month)

A. Hardware Contribution:

Boolean expression for TOP event: $T = \bigcup_{k=1}^{16} E_k$

Unavailability $Q(T) = \sum_{\substack{k=1 \\ k\neq 5}}^{16} Q(E_k)$

On average not more than 4 shutdown are expected in a year. To be on safe side, we assume 1 shutdown in a month.

$Q_{ROD} = 0.0393$

B. Test and Maintenance Contribution:

i) Test and maintenance unavailability due to instrument channels [5] $= 1.2 \times 10^{-5}$

ii) For mechanicalsystem 'Drop Test', to check the time to fall is conducted. Assuming it can take a minimum of 7.5 min and a 2 hr. maximum time, the lognormal average is 0.72 hrs. and unavailability due to testing is (5) $= 1.0 \times 10$

iii) The maintenance downtime has a lognormal average of 7 hrs. (a range of 0.5 hr. to 24 hrs.) and assuming maintenance frequency to be once in 4.5 months on average (associated with 90 range of 1 month to 12 months) the unavailability is $= 2.1388 \times 10^{-3}$

C. Common Cause Failure Contribution:

As has been discussed in Appendix C,

Common cause failure unavailability

$$Q_{CM} = \sqrt{Q(E2).Q(E2).Q(E5)}$$

Common cause failure unavailability $= 8.03 \times 10^{-7}$

D. Total unavailability based on 1 mo. testing and maintenance schedule $= 4.245 \times 10^{-2}$

E. Computation of Confidence Bounds on TOP Event:

By Taylor series expansion of unavailability expression and taking second moment of both sides it can be shown that

$$\mu_2 (Q_T) = \sum_{\substack{i=1 \\ i\neq 2,6}}^{16} \mu_2(Q_i) + \mu_2(\text{testing}) + \mu_2 (\text{maintenance})$$

$$+ \mu_2(Q_2) + \frac{3}{2} Q_2^{\frac{1}{2}} \mu_2(Q_2)$$

For E16 because of lack of information only point estimate of unavailability is available therefore dispersion information is not included in calculating $\mu_2(Q_T)$. Substituting appropriate values:

$$\mu_2(Q_T) = 2.3446 \times 10^{-3}$$

hence, Standard deviation $\sigma_T = 0.0232943$

E1. Confidence bounds using Tchebycheff inequality [Eqns. 3.9 and 3.10]:

Lower bound, $L_{0.05} = 0.0$

Upper bound, $U_{0.95} = 0.1468151$

E2. Confidence bounds assuming a lognormal distribution for TOP event [Eqns. 3.12 and 3.13]:

Lognormal parameters are: $\mu = -3.1594284$ and $\sigma = 1.3552$

Lower bound $= 4.7605 \times 10^{-3}$

Upper bound $= 0.3785$

E3. Confidence bounds assuming a Weibull distribution for TOP event. Weibull parameter β and α can be computed knowing mean and μ_2.

$\beta = 1.945$

$\alpha = 0.0478746$

hence,

$L_{0.05} = 0.010401$

$L_{0.95} = 0.08414$

3.4 FAULT TREE QUANTIFICATION FOR LPSR:

Fault tree of a single LPSR is shown in Fig. 3.2 and is used here for determining TOP event unavailability using methods discussed in Sections 3.1 and 3.2. A scheduled testing and maintenance period of 30 days (720 hrs) is assumed and Common cause failures are identified and their contribution

to the overall unavailability is computed using techniques discussed in Appendix C. Confidence interval and point estimates are computed in Section 3.4.1 and results along with data used and the results of Monte-Carlo simulation of LPSR and Fault tree of LPSR are presented in Tables 3.2.

3.4.1 COMPUTATION OF POINT ESTIMATES OF THE UNAVAILABILITY OF A SINGLE LPSR:

A. Hardware Contribution:

Boolean expression for TOP event

$$= T = (E11) \cap (E12) \cup \left(\bigcup_{k=1}^{23} E_k \right)$$

$$k \neq 11,12,15,22,23$$

Unavailability $Q(T) = Q(E11).Q(E12)$

$$+ \sum_{\substack{k=1 \\ k \neq 11,12,15,22,23}}^{23} Q(E_k)$$

On average not more than 4 shutdown are expected in a year. As LPSR is a backup system it will be called upon operate still less frequently. However, a frequency of 1 per month is assumed to include events defined as failure per demand.

$$Q = 0.0723944$$

B. Testing and Maintenance Contribution:

Same as for EMSR $Q = 3.1388 \times 10^{-3}$

C. Common Cause Failure Contribution:

Pair of events causing common cause failure are : (E15, E18), (E20,E22) and (E21,E23)

$$Q_{CM} = Q(E15)^{3/2} + Q(E20)^{3/2} + Q(F21)^{3/2}$$
$$= 2.7 \times 10^{-8} + 3.9540 \times 10^{-5} + 6.49 \times 10^{-3}$$

Hence $Q_{CM} = 6.5307 \times 10^{-3}$

D. Total Unavailability of a Single LPSR = 8.206×10^{-2}

E. Computation of Confidence Bounds on TOP Event:

Using Taylor's series expansion of unavailability expression and taking second moment of both sides it can be shown that

$$\mu_2(Q_T) = \sum_{\substack{i=1 \\ i \neq 11,12,15,22,23}}^{23} \mu_2(Q_i) + Q_{12} \cdot \mu_2(Q_{11})$$
$$+ Q_{11} \cdot \mu_2(Q_{12}) + \frac{3}{2} Q_{15}^{\frac{1}{2}} \mu_2(Q_{15})$$
$$+ \frac{3}{2} Q_{20}^{\frac{1}{2}} \mu_2(Q_{20}) + \frac{3}{2} Q_{22}^{\frac{1}{2}} \mu_2(Q_{22})$$
$$+ \mu_2 \text{ (testing and maintenance)}$$

where subscript i denotes event Ei.

Events E1, E2 lack information on the dispersion of unavailability and therefore they are not included in calculating $\mu_2(T)$. Substituting appropriate values:

$\mu_2(Q_T) = 0.0118782$

Variance $(Q_T) = 5.1444 \times 10^{-3}$

hence, Standard deviation $\sigma_T = 0.0717249$

E1. Confidence Bounds Using Tchebycheff Inequality [Eqn. 3.9 and 3.10]:

Lower bound, $L_{.05} = 0$

Upper bound, $U_{.95} = 0.394593$

E2. Confidence Bounds Using a Lognormal Distribution for TOP event [Eqn. 3.12 and 3.13]:

Lognormal parameters are: $\mu = -2.5003046$,

$\sigma = 0.5327093$

Lower bound, $L_{.05} = 0.03472$

Upper bound, $U_{.95} = 0.193932$

E3. Confidence Bounds Using a Weibull Distribution for TOP event [Eqns. 3.14 and 3.15]:

Weibull distribution parameters are: $\beta = 1.153$,

$\alpha = 8.62 \times 10^{-2}$

Lower bound, $L_{.05} = 6.5575 \times 10^{-3}$

Upper bound, $U_{0.95} = 0.22324$

3.5 COMPUTATION OF SYSTEM UNAVAILABILITY:

Substituting in the unavailability expression for the EMSR and LPR system given in sections (2.1.1) and (2.2.1) respectively, the following values we obtain system unavailability due to chance failure and testing and maintenance outages,

$q_{IC} = 3 \times 10^{-3}$/demand (obtained from ref. [22])

$q_{} = 4.55 \times 10^{-2}$/demand (from Table 3.10)

Mean unavailability of EMSR system = 2.39×10^{-2}/demand

and $q_{LP} = 0.1$/demand

Mean unavailability of LPR shut-off system = 0.0158/demand.

The computed mean unavailabilities are for a fault exposure time of 720 hrs. with the assumption that one shut-down may be expected during this period. Since, on average four shutdowns are expected in a year the values obtained are slightly conservative. Since only few basic components have their failure rate expressed as unavailability per demand, we can safely express system unavailability in terms of system failure rate. Hence,

$$\lambda_{EMSR,\ system} = 3.319 \times 10^{-5}$$

$$\lambda_{LPR,\ system} = 2.1944 \times 10^{-5}$$

Table 3.1A: Monte-Carlo Simulation of Electromechanical Shutdown Rod for Time Required to Fall to the Support SP.

Sample size : 1000

Parameter: Time required by EMSR to fall to support SP after release of magnetic clutch, T in sec.

NB: The frequency distribution of T is shown in Fig. 3.3

Description of Parameter measures	Assumed standard deviation of normal distribution of component dimension as a fraction of design values (as mean)				
	0.5	1.0	2.0	4.0	6.0
1. 5 percentile lower limit on T, sec.	1.66236	1.64391	1.57904	1.55183	1.50972
2. 95 percentile upper limit on T,	1.70149	1.72282	1.82189	1.88222	2.04729
Normal Distribution M.L.Estimates					
3. Mean of T	1.68203	1.68292	1.69207	1.69975	1.72363
4. Standard deviation on T	0.01208	0.024615	0.0742899	0.1020382	0.1731981
Lognormal distribution M.L.Estimates					
5. Median of T	1.68199	1.68275	1.69046	1.69675	1.71560
6. Standard deviation on T	0.0121457	0.0341987	0.0788249	0.1006	0.1641937
7. Parameter σ	0.00719	0.01438	0.04361	0.05915	0.09506
Weibull Distribution Estimates					
8. Shape parameter β	174.80443	86.744343	28.429167	21.070682	13.35
9. Scale parameter α	1.6856826	1.6899392	1.708477	1.7173204	1.74
10. Mean of T	1.68568	1.6803572	1.6743074	1.6718	1.67388
11. Standard deviation on T	0.0220753	0.0172236	0.1046223	0.1441924	0.1516497
12. Recommended Distribution	NORMAL DISTRIBUTION				
13. Unavailability [Probability that the time required to fall to support SP exceeds 2 secs.]	0.5×10^{-27}	0.5×10^{-13}	0.5×10^{-5}	1.6×10^{-3}	0.0548

Table 3.1 B: Data on failure rate or unavailability of Basic Events of Fault Tree of Electromechanical Shutdown Rod.

EVENT	EVENT DESCRIPTION	Failure rate distribution	Failure rate distribution parameters	Mean failure rate/10^6 hr
E1	Shaft 2 locked in bearings[1]	Weibull	$\beta = 1.045$, $\alpha = 1.235 \times 10^{-6}$	0.609
E2	Gears G2 and G3 locked[2]	Weibull	$\beta = 1.437$, $\alpha = 0.132 \times 10^{-6}$	0.12
E3	Gears G1 and G2 locked	Weibull	$\beta = 1.437$, $\alpha = 0.132 \times 10^{-6}$	0.12
E4	Shaft 3 locked in bearings[1]	Weibull	$\beta = 1.045$, $\alpha = 1.235 \times 10^{-6}$	0.609
E5	Gears G2 and G3 locked[2]	Weibull	$\beta = 1.437$, $\alpha = 0.132 \times 10^{-6}$	0.12
E6	Rope is stucked in a groove on drum			
E7	Shaft 1 fails to rotate[1] (locked in bearings)	Weibull	$\beta = 1.405$, $\alpha = 1.235 \times 10^{-6}$	0.609
E8	Shaft 4 fails to rotate[1] (locked in bearings)	Weibull	$\beta = 1.405$, $\alpha = 1.235 \times 10^{-6}$	0.609
E9	Shaft 5 fails to rotate[1] (locked in bearings)	Weibull	$\beta = 1.405$, $\alpha = 1.235 \times 10^{-6}$	0.609
E10	Instrument channel-failure to operate	Weibull	$\beta = 0.883$, $\alpha = 1.515 \times 10^{-6}$	1.612
E11	Instrument channel-shift in calibration	Weibull	$\beta = 0.883$, $\alpha = 4.54 \times 10^{-6}$	48.33
E12	Spring SR of magnetic clutch fail to release (a pair)	Weibull	$\beta = 1.766$, $\alpha = 0.48 \times 1 \times 10^{-6}$	0.42
E13	Accelerator spring fails to release	Weibull	$\beta = 0.588$, $\alpha = 1.56 \times 10^{-8}$	2.4106×10^{-2}
E14	Support SP breaks	Weibull	$\beta = 1.766$, $\alpha = 4.2E-8$	2.4×10^{-2}
E15	Rod fails to reach support in 2 secs. (unavailability per demand)	Point estimate		
E16	Testing and maintenance of Instrument channels (unavailability)	Lognormal	$\mu = -5.539563$, $\sigma = 0.630$	1.2×10^{-5}
E17	Testing of mechanical system (unavailability)	Lognormal	$\mu = -7.2721$, $\sigma = 0.84017$	1.0×10^{-3}
E18	Maintenance of mechanical system (unavailability)	Lognormal	$\mu = -5.3368$, $\sigma = 1.173$	2.1388×10^{-3}

Foot notes to Table 3.1B:

1. Event shaft fails to rotate or shaft locked in bearing includes two independent events, viz ., event A and event B as shown below:

   ∴ Shaft locked in bearing

   = [Failure of Bearing] OR [Failure of Shaft]

   Event A Event B

2. E2 and E5 will lead to Common mode failure. TOP event will occur through failure modes initiated by either E2 or E5. Because E2 and E5 are same both the failure modes will occur simultaneously and thus lead to a higher unavailability, and appropriate term will have to be included while computing TOP event unavailability. It has to be noted that one of the two events E2 and E5 is redundant.

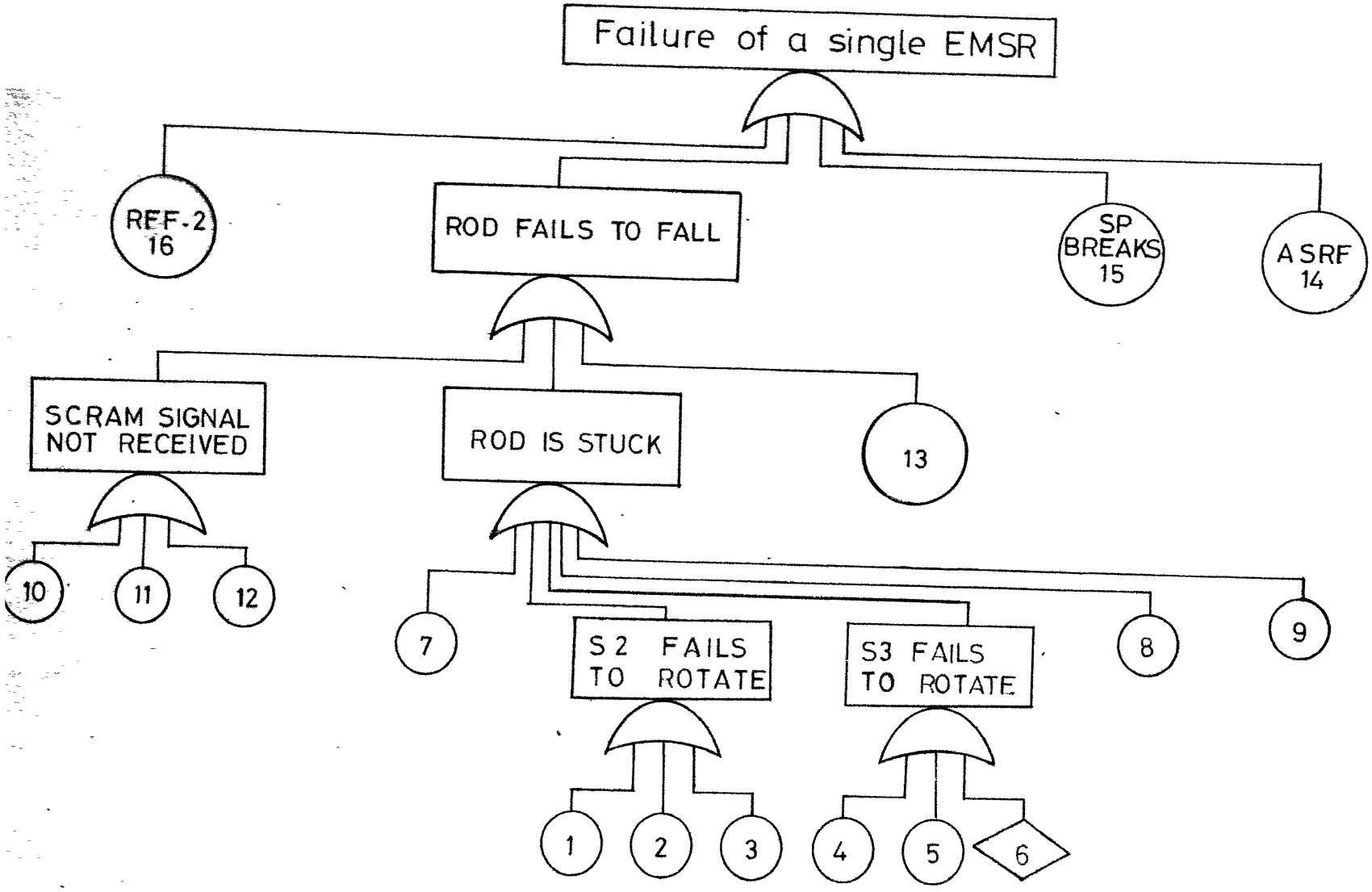


Fig. 3.1 Fault tree of a single EMSR
(For the description of events refer to Table 3.1B)

Table 3.1.C: Monte-Carlo Simulation of Fault-Tree of EMSR

TOP event unavailability expression is,

$$Q(T) = \sum_{\substack{k=1 \\ k\neq 5}}^{16} Q(E_k) + Q(E17)+ (E18)+Q(E19)+ Q(E2).Q(E2).Q(E5)$$

where E16 : Testing and maintenance of instrument channels
E17 : Testing of mechanical system
E18 : Maintenance of mechanical system

Sample size = 1200
Parameter : Unavailability of a single EMSR
Fault Exposure Time : 720 hrs (1 month)

Description of Parameter measures	Values
1. 5 Percentile lower limit on Q(T)	0.01524
2. 95 Percentile upper limit on Q(T)	0.13469
Normal Distribution M.L.Estimates	
3. Mean of Q(T)	0.05536
4. Standard deviation on Q(T)	0.04459
Lognormal Distribution M.L. Estimates	
5. Median of Q(T)	0.04337
6. Standard deviation of T	0.0423606
7. Parameter σ	0.68432
Weibull Distribution Estimates	
8. Shape parameter β	1.866
9. Scale parameter α	0.051243
10.Mean of Q(T)	0.045513
11. Standard deviation on Q(T)	0.0250216
12. Recommended Distribution	WEIBULL

NB: The frequency distribution of Q(T) is shown in Fig. 3.4).

Table 3.2A: Monte-Carlo Simulation of Liquid Poison Shutoff Rod for Time Required to Fill the Liquid Poison Rod:

Sample Size = 1000

Parameter: Time required by LPSR to fill LPR, T sec.

NB: The frequency distribution of T is shown in Fig. 3.5 .

Description of parameter measures	Values	Remarks
1. 5 percentile lower limit on T	2.82735	
2. 95 percentile upper limit on T	3.48055	
Normal Distribution M.L. Estimates		
3. Mean of T	3.15597	Standard deviation of He-gas pressure in cylinder, LHT and GHT = 5 percent of mean pressure in respective tanks. [32]
4. Standard deviation on T	0.19938	
Lognormal Distribution M.L.Estimates		
5. Median of T	3.14956	
6. Standard deviation on T	0.2025705	
7. Parameter σ	0.06412	
Weibull Distribution Estimates		
8. Shape parameter β	19.567	
9. Scale parameter α	3.2163289	
10. Mean of T	3.13	
11. Standard deviation on T	0.1942566	
12. Recommended distribution	LOG NORMAL DISTRIBUTION	
13. Unavailability [Probability that T exceeds specified time)		
i) specified time = 6 sec.	$< 0.5 \times 10^{-15}$	Except when specific time is 4 secs. the unavailability of time bound event is negligible.
ii) specified time = 5 sec.	$< 0.5 \times 10^{-10}$	
iii) specified time = 4 sec.	$< 0.5 \times 10^{-5}$	

Table 3.2B: Data on failure rate or unavailability of basic events of fault tree of Liquid Poison shut-off rod.

Event	EVENT DESCRIPTION	Failure rate distribution	Failure rate distribution parameters	Mean failure rate per 10^6hr.
E1	Failure to fill LPR in specified time			10^{-5}/demand
E2	LPR ruptures[1]			
E3	Statistical fluctuation causing[2] PG PL + h_L (unavailability)	point estimate		5×10^{-8}/demand
E4	Pipe segments P2 or P3 rupture or elbows leak (No.3 elbows)	Weibull	$\beta = 0.588$, $\alpha = 4.68\times10^{-6}$	7.2
E5	Insufficient liquid in LPT (high pressure tank failure)[5]	Weibull	$\beta = 3.43$, $\alpha = 0.089\times10^{-6}$	0.08
E6	Valve V2 (check valve) leaks	Weibull	$\beta = 1.851$, $\alpha = 3.75\times10^{-8}$	1.25×10^{-2}
E7	Pipe segments P5 or P6 or P7 or P8 rupture or elbows (10) leak	Weibull	$\beta = 0.588$, $\alpha = 1.56\times10^{-5}$	24.0
E8	V1 leaks (control solenoid valve)	Weibull	$\beta = 1.851$, $\alpha = 3.75\times10^{-8}$	1.25×10^{-2}
E9	Plunger of V1 is plugged	Weibull	$\beta = 1.851$, $\alpha = 11.25\times10^{-6}$	3.75
E10	Plunger of V2 is plugged	Weibull	$\beta = 1.851$, $\alpha = 11.25\times10^{-6}$	3.75
E11	Valve V3 leaks[3]	Weibull	$\beta = 1.851$, $\alpha = 3.75\times10^{-8}$	1.25×10^{-2}
E12	Valve V4 leaks[4]	Weibull	$\beta = 1.851$, $\alpha = 3.75\times10^{-8}$	1.25×10^{-2}

contd...

Event	EVENT DESCRIPTION	Failure rate distribution	Failure rate distribution parameters	Mean failure rate per 10^6 hr.
E13	Pressure sensor fails	Weibull	$\beta = 2.72,\ \alpha = 4.497 \times 10^{-6}$	4.0
E14	Valve V6 fails closed (plugged)	Weibull	$\beta = 1.851, \alpha = 11.25 \times 10^{-6}$	3.75
E15	Valve V3 leaks[3]	Weibull	$\beta = 1.851, \alpha = 3.75 \times 10^{-8}$	1.25×10^{-2}
E16	Pressure sensor fails	Weibull	$\beta = 2.72,\ \alpha = 4.497 \times 10^{-6}$	4.0
E17	Valve V7 leaks			
E18	Valve V3 leaks[3]	Weibull	$\beta = 1.851, \alpha = 3.75 \times 10^{-8}$	1.25×10^{-2}
E19	Valve V4 leaks[4]			
E20	Instrument channel-failure to operate	Weibull	$\beta = 0.833, \alpha = 1.515 \times 10^{-6}$	1.612
E21	Instrument channel-shift in calibration	Weibull	$\beta = 0.833, \alpha = 4.54 \times 10^{-5}$	48.33
E22[6]	Same as E20	Weibull	$\beta = 0.833, \alpha = 1.515 \times 10^{-6}$	1.612
E23[6]	Same as E21	Weibull	$\beta = 0.833, \alpha = 4.54 \times 10^{-5}$	48.33

Foot notes to Table 3.2B:

1. Rupture of LPR is same as rupture of a pipe segment and has a very small chance failure rate ($\lambda \sim 9.22 \times 10^{-9}$ per section) and is therefore neglected.

2. The event of interest is $PG > PL + h_L$
Where PG is pressure of He-gas in GHT, PL is pressure of He-gas in LHT and h_L is pressure of liquid column head in LHT and pipe P2 at point A. It is assumed that PG, PL and h_L are Normally distributed random variable having a Standard deviation of 5 percent of the mean value [32].

PG: μ_G = mean = 2.1 Kgf/cm^2, σ_G = Standard deviation = 0.105

PL: μ_L = 1.75 Kgf/cm^2, σ_L = 0.0875

h_L: h_L = 1.26 Kgf/cm^2,

event $PG > PL + h_L$ $\quad PG - PL > h_L$

$Pr[PG-PL > h_L] = Pr[X > h_L]$

where X is new random variable having $\mu = 0.35$, $\sigma = 0.137$.

It can be shown that $Pr[X > 1.26] = 5 \times 10^{-8}$

3. Events E11, E15 and E18 although same cannot be off-hand declared redundant. Only E15 and E18 are redundant. However, because they simultaneously initiate different failure modes of TOP event common mode failure contribution has to be considered. Event E11 being compounded with E12, and each being a low probability event, can be treated to have negligible effect-Common mode failure contribution of E15 and E18 is to be included.
4. Events E12 and E19 although same can neither be treated as redundant or as initiating common cause failure because progress of failure chain initiated by E12 is constrained by event E11.
5. Apart from tank failure which will cause loss of liquid poison; in all other possible circumstances if there is liquid in LHT, however little, it will be definitely available at point A. During shut-down the liquid poison in LHT drains and is recirculated by feed pumps back to LHT where its level is monitored by level sensors. Therefofe E5 can exist after shutdown due to failure of feedpumps or level sensors or during scheduled testing and maintenance period. It is only during maintenance period that E5 can occur unavailability due to which is considered in E25 and E26.
6. Events(E20 and E22)and (E21 and E23) are redundant. Common cause contribution of E20 and E22 and that of E21 and E23 has to be included.

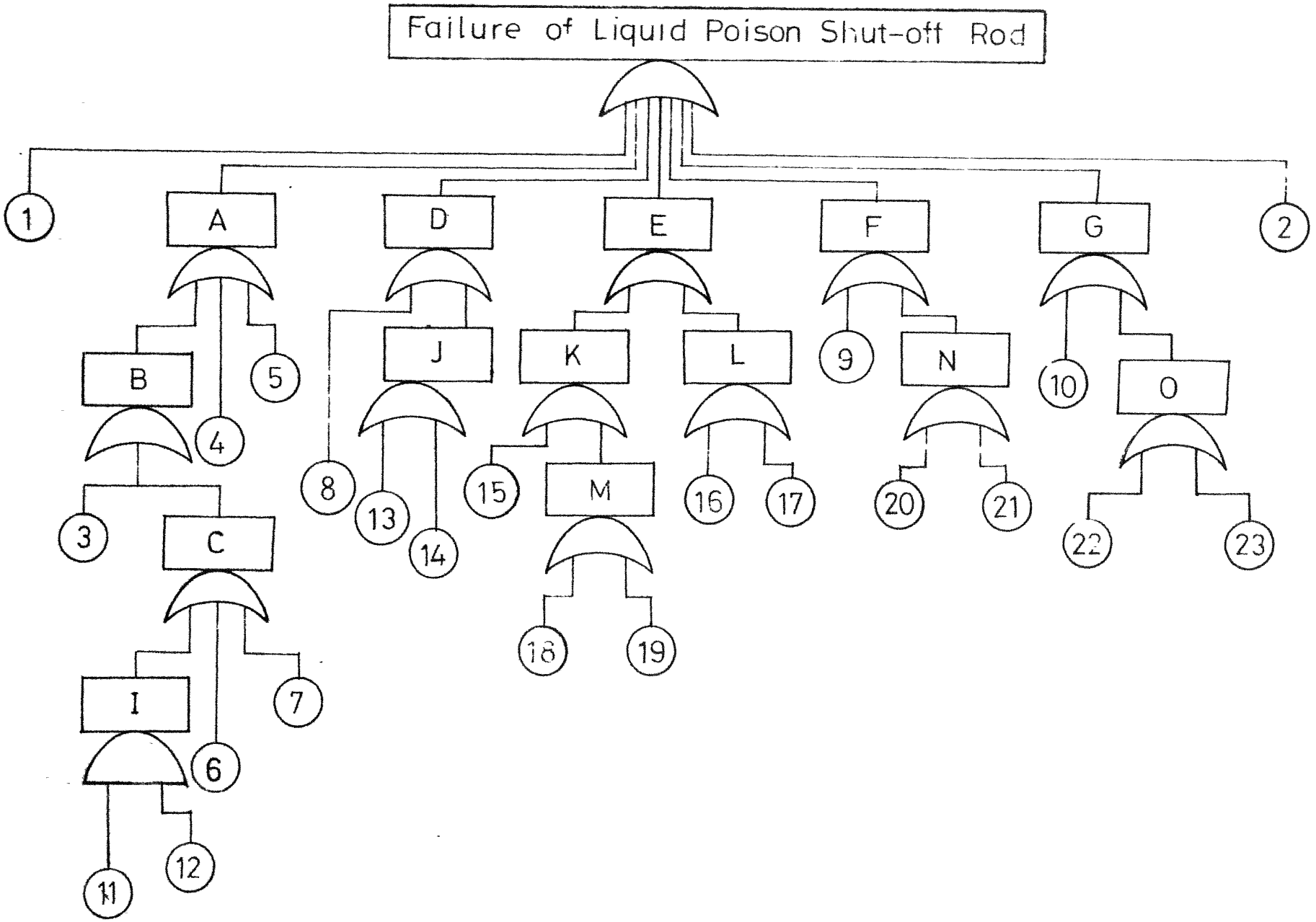


Fig.3·2 Fault tree of a single LPR
(For the description of events to refer to Table 3·2 B)

LEGEND OF FIG. 3.2 :

A	Liquid Poison Unavailable at Point A (Fig. 2.3)
B	He-gas pressure in GHT, PG, is greater than the total head of liquid at point A, P2+PL (PL is He-pressure in LHT).
C	He-pressure in LHT is below the specified limit.
D	He-pressure in GHT is below the specified limit.
E	He-pressure in Booster cylinder is below the specified limit.
F	Valve V1 fails closed
G	Valve V3 fails closed
I	Valves V3 and V4 leak
J	Failure of differential pressure controller
K	Low pressure side valve leakage
L	High pressure controller fails
M	Valves V3 or V4 leak
N,O	Scram signal not received.

NB: For description of other events refer to Table 3.2B.

Table 3.2C: Monet-Carlo simulation of fault tree of LPSR.

TOP event unavailability is given by,

$$Q(T) = \sum_{\substack{k=1 \\ k\neq 11,12,15,22,23}}^{23} Q(E_k) + Q(E11).Q(E12)$$

$$+ Q(E24) + Q(E25) + Q(E26) + Q(E18)^{3/2}$$

$$+ Q(E20)^{3/2} + Q(E21)^{3/2}$$

where E24: Testing and maintenance of instrument channels
E25: Testing of fluidic system
E26: Maintenance of fluidic system
Sample size : 1200
Parameter: Unavailability of a single LPSR
Fault Exposure Time : 720 hrs. (1 month)

Description of Parameter Measure	Value
5 percentile lower limit on Q(T)	0.03670
95 percentile upper limit on Q(T)	0.25937
Normal Distribution M.L. Estimates	
Mean of Q(T)	0.11794
Standard deviation on Q(T)	0.08717
Lognormal Distribution M.L. Estimates	
Median of Q(T)	0.09661
Standard deviation of Q(T)	0.079934
Parameter σ	0.81890
Weibull Distribution Estimates	
Shape parameter β	2.0798
Scale parameter α	0.11382
Mean of Q(T)	0.1008388
Standard deviation on Q(T)	0.05049
Recommended Distribution	WEIBULL

The frequency distribution of Q(T) is shown in Fig. 3.6.

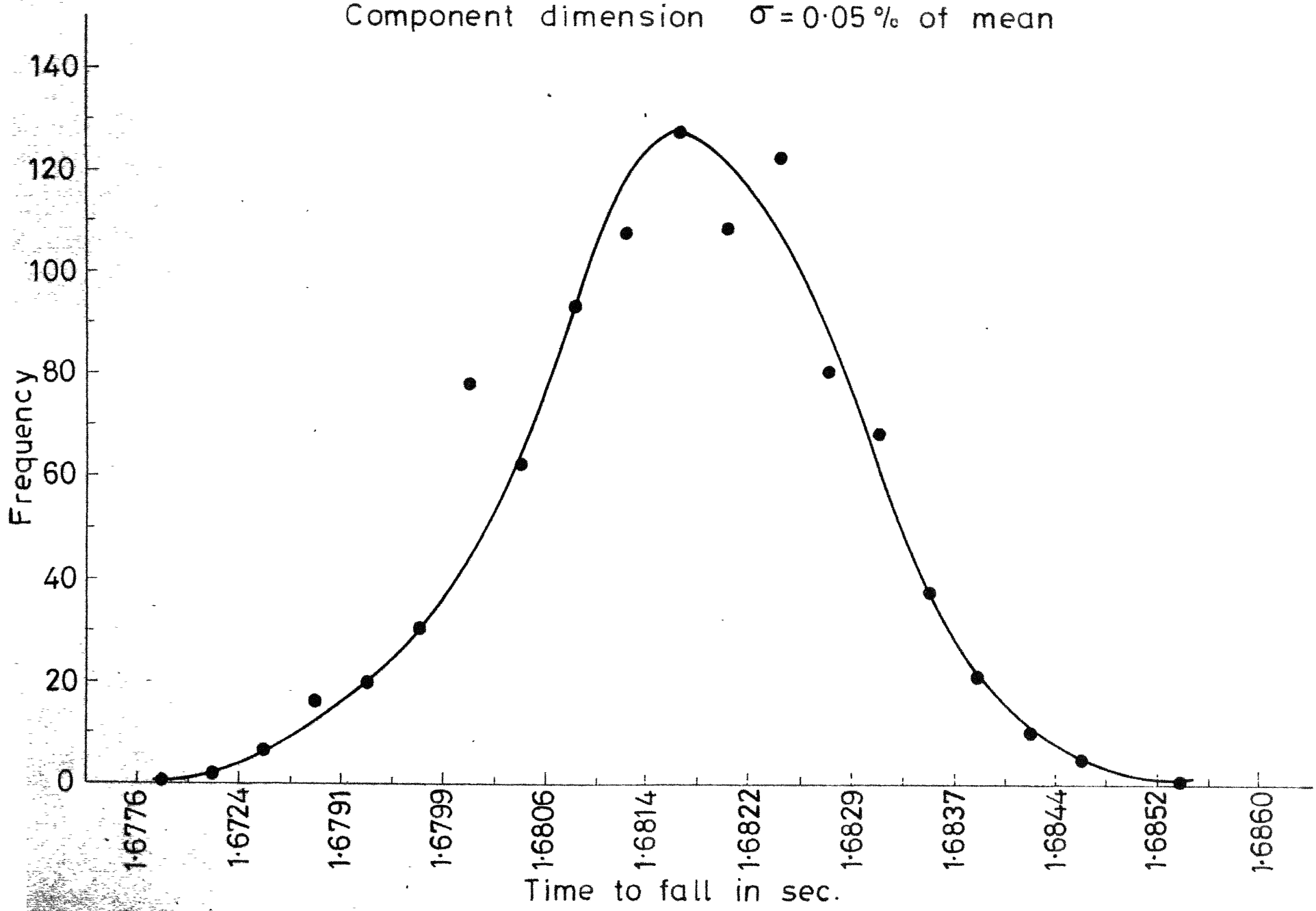


Fig. 3·3 EMSR : Monte-Carlo simulation of EMSHUT

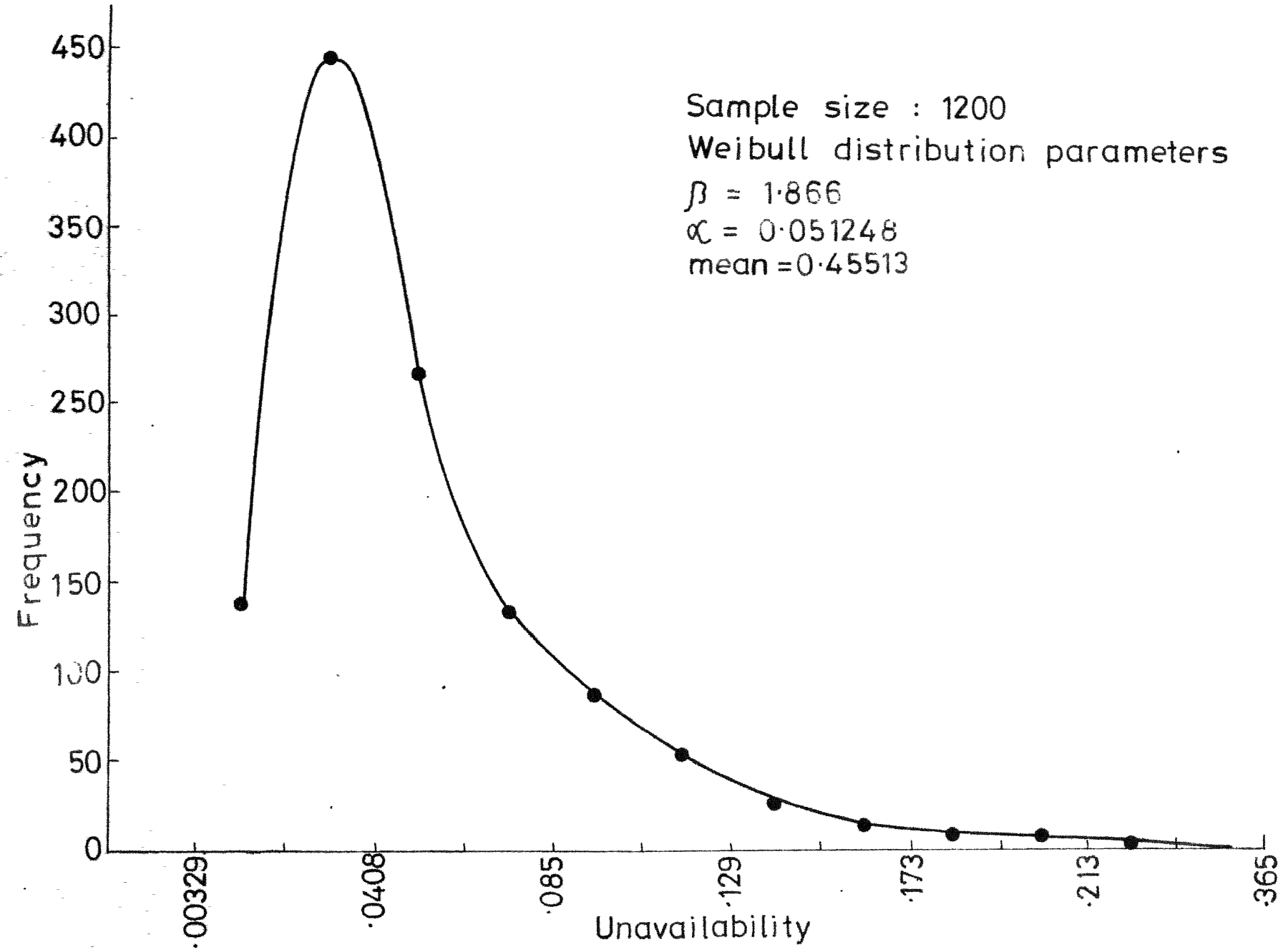


Fig. 3·4 EMSHUT : Unavailability frequency distribution

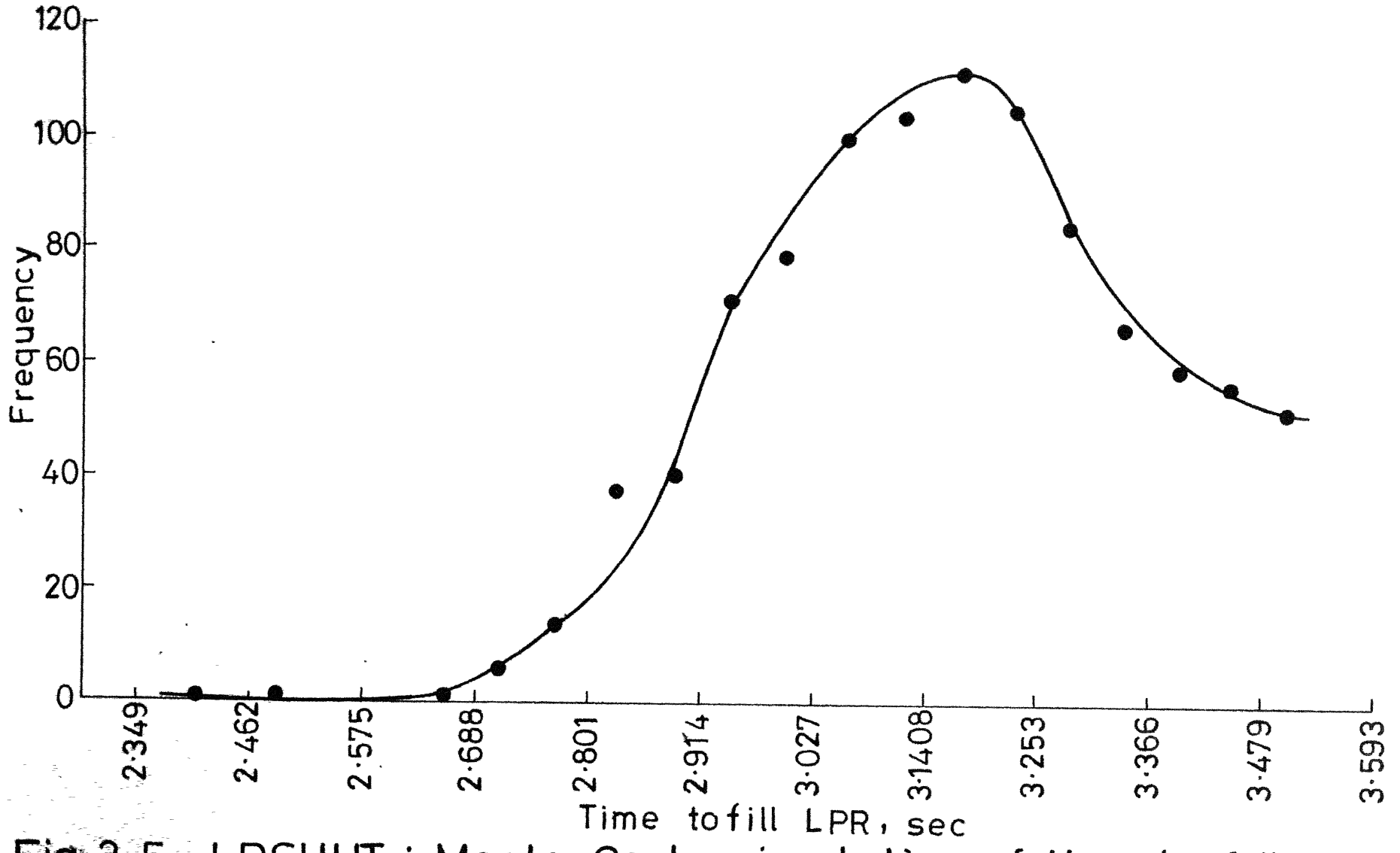


Fig.3.5 LPSHUT : Monte-Carlo simulation of time to fill LPR

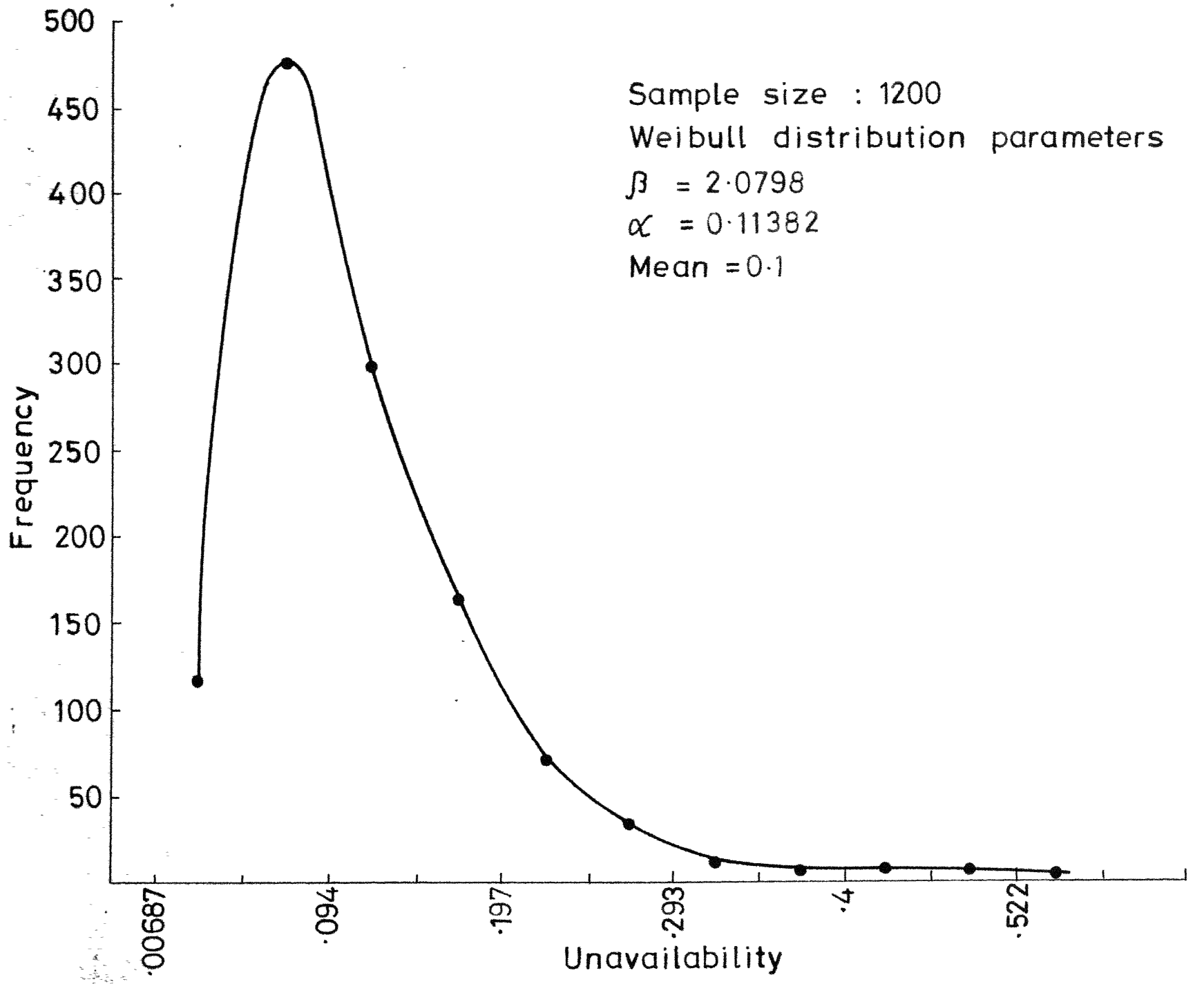


Fig. 3·6 LPSHUT : Unavailability frequency distribution

CHAPTER 4

REACTOR SHUT-DOWN SYSTEM RELIABILITY ESTIMATION

In Chapter 3, unavailability of a single, EMSR and LPR has been computed and therefrom the failure rate of these systems. This failure rate is to be interpreted as chance failure rate and was obtained by assuming basic component failure mode to be chance failure therefore using constant failure rate values for the time period of interest. Such an assumption is justified if 'ideal repair on failure' or to some extent 'ideal preventive maintenance' is undertaken. In addition to chance failure the component will be subjected to aging and this can have significant effect on the component unavailability over a span of 1 year. It is therefore meaningful to include expected deterioration in basic component life expectency over a period of 1 year in reliability estimation.

4.1 TIME DEPENDENT FAILURE RATE:

If a component failure can take place due to different physical mechanisms viz., chance failure and wear out the component hazard rate is given by the sum of the hazard rates due to the chance failure and wear out. Hence,

$$h(t) = h_c + h_w(t) \qquad (4.1)$$

where $\bar{h}_c$ is chance failure rate (constant)

$h_w(t)$ is wearout hazard rate

$h(t)$ is component hazard rate

$h_w(t)$ is hazard function of time to failure distribution. In reliability practice Weibull is the most popular time to failure distribution[26,27] because it is flexible and experience substantiates its use. Hazard function for Weibull distribution is given by

$$h(t) = \frac{\beta}{\alpha^{\beta}} t^{\beta-1} \qquad (4.2)$$

where β is shape parameter and α location parameter. Because wearout results in progressive deterioration $h(t)$ has to be a monotonically increasing function hence $\beta > 1$.

The problem inherent in applying this concept to the present problem is that no data is available in choosing a value of β and α. Life expectancy of most of the components is based on fatigue failure and a value of β around 1.5 is used [27]. Experience reveals that because of environment and working conditions at site mechanical components fail long before their predicted life expectancy, e.g., less than 10% of all roller bearings reach their predicted life. Japanese research in roller bearings show a reduction of life of 40 to 60% of rated life in low particle and moisture

concentration environment [27]. Moreover, for highly reliable components large value of β is chosen. Based on the considerations above, in the absence of any specific information, $\beta = 2$ is chosen for the sake of analytical simplicity as it leads to a linear hazard rate.

To find α a constraint is applied that at the end of a specific period the component should have a reliability R. Such a specification can be made even if the mechanisms that can lead to failure of component is not known. Reliability for Weibull distribution associated component is given by

$$R(t) = \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right] \tag{4.3}$$

For $\beta = 2$

$$\alpha = t\left[\ln \frac{1}{R(t)}\right]^{\frac{1}{2}} \tag{4.4}$$

using this concept one can specify required component reliability to assure a given system reliability. R(t) is termed here as 'target reliability', under aging.

4.2 TIME DEPENDENT SYSTEM RELIABILITY:

Knowing thus time dependent failure rate $h_i(t)$ for i-th component or critical path, the system hazard rate can be computed by summation property of hazard rate for a series system, hence

$$h_s(t) = \sum_i [h_{ci} + h_{wi}(t)] \tag{4.5}$$

where $h_s(t)$ is system hazard rate. We can now compute equivalent chance hazard rate λ_s and equivalent Weibull parameters α_s and β_s. The unavailability of EMSR or LPRS at any time t is given by,

$$q_s(t) = 1 - e^{-\lambda_s t} + 1 - \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right] \qquad (4.6)$$

For rare events λ_s is usually small, hence

$$q_s(t) = \lambda_s t + 1 - \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right] \qquad (4.7)$$

Using the value of $q_s(t)$ in equations (2.1) and (2.3) one can compute unavailability of the EMSR system and that of LPRS system. The reliability of reactor shutdown system is given by,

$$R_{RSS}(t) = R_{EMSR}(t) + Q_{EMSRS}(t) \cdot R_{LPRS}(t)$$

where R(t) : reliability of subscripted system at time t

Q(t) : 1 - R (t)

and subscripts RSS : Reactor shutdown system

EMSRS : Electromechanical shutdown rod system

LPRS : Liquid Poison rod shut-off system.

Results are presented in Table (4.1).

Table 4.1: Time dependent unavailability analysis.

NB : 1. R(t) : Target reliability at the end of a year (t = 8760 hrs.) of a basic component under aging alone.

2. Number of basic components Affected by aging: 12 in EMSR, 16 in LPR

3. Weibull distribution shape parameter $\beta = 2$

Target Reliability R(t=8760 hrs)	Weibull distribution scale parameter α	EMSR System Q(t=720 hrs)	LPR system Q(t=720 hrs)	Combined Q(t=720hr
0.90	26987.6	0.0324	0.0271235	$8.78 \times 10^{-}$
0.99	87380.586	2.47×10^{-2}	1.8885×10^{-2}	$4.17 \times 10^{-}$
0.999	276947.88	2.398×10^{-2}	1.5908×10^{-2}	3.815×10
0.9999	876000.0	2.39×10^{-2}	0.0158	3.766×10

CHAPTER 5

CONCLUSIONS AND DISCUSSION

5.1 CONCLUSIONS:

The objective of the present study has been to estimate the unavailability of reactor shut-down system of a CANDU-reactor. The contribution of the present work is incorporation of the following aspects into the unavailability analysis of reactor shutdown system:

1. Choice of Weibull distribution for failure rate of basic components.
2. Study of the effect of time constraint performance on system unavailability.
3. Inclusion of the unavailability contribution of mechanical and fluidic systems.
4. Study of the effect of aging of basic components on system unavailability.

5.1.1 The purpose of assigning a distribution to failure rate data is to obtain an estimate of location parameter with as low a variance as possible without loosing information on the shape of distribution. As has been mentioned in Appendix C, both Lognormal and Weibull distribution were tried on the field data available and it is found that for all the

components Weibull distribution gives a lower variance than Lognormal distribution; both of them resulting in almost equal value of location parameter. Therefore, in present study Weibull distribution has been used to represent failure rate data.

5.1.2 Both, the EMSR and LPSR are required to perform their function within specified time. The time taken to operate successfully by EMSR and LPSR is computed using mathematical models described in Appendices A,B and the Monte Carlo simulation results are tabulated in Tables 3.1A and 3.2A respectively. The deterministic time required for successful operation of EMSR and LPSR is 1.68 and 3.15 seconds, and specified upper limit on the time of operation is 2.0 and 6.0 seconds. As can been seen from Table 3.1A the time constrained unavailability of EMSR is negligible if the relative dispersion on component dimensions is less than 2 percent, which is the usual case. Similarly Table 3.2A depicts that time constrained unavailability of LPSR is negligible. Therefore, it can be safely concluded that with the present day manufacturing practices the time constraint unavailability is negligible if the shut-down system is designed to operate two times faster than the required speed.

5.1.3 As has been mentioned in Chapter 1, major contention of the present study has been that the failure of mechanical and

and fluidic systems will contribute significantly towards the unavailability of reactor shutdown system. Results of present study support this assertion. Table 5.1 compares the results obtained with those reported by WASH-1400 and it can be seen that the affect of mechanical and fluidic system unavailability is to increase the system unavailability by an order of magnitude.

5.1.4 From the results presented in Table 4.1 the effect of aging of components on system unavailability is obvious. However, if components are designed to have a reliability of 0.9999 at the end of 8760 hrs. (1 year) the affect of aging is negligible.

5.2 SPECIFYING MINIMUM LEVEL OF REDUNDANCY:

In a m/n (a minimum of m components should operate) redundant system depending upon the value of the unavailability of a single component, the system reliability can be either greater or lesser than component reliability. However, it is desirable that system reliability be greater than the component reliability. For a specified value of m, and various values of component unavailability, values of n can be calculated such that above mentioned criterion is satisfied. Table 5.2 tabulated desired redundancy for m = 12 and 46. The information contained in this table can be used as a design aid.

5.3 PROPOSAL FOR FURTHER WORK:

In the present work fault tree model of CANDU protection system is developed and has been used to estimate the unavailability of the protection system on the basis of specified design, systems logic and testing and maintenance procedures. No attempt has been made to conduct postmortem of design and maintenance procedure adequacy. The present work can be extended to include:

1. Analysis of partial insertion of rod.
2. Optimum decision on testing and maintenance procedures and the value of n.
3. Reliability analysis against inadvertent trips.

5.3.1 To shutdown a reactor a definite amount of negative reactivity is required to be inserted. This poison is distributed in m rods so as to achieve an effective poison introduction throughout the core. Usually, m rods contain more poison than is needed for reactor trip. Moreover, since stuck-up rod and partial insertion accompany poison insertion they are not failures in a strict sense. Defining the TOP event so as to include amount of poison inserted instead of number of rods will produce more realistic results. Furthermore, four shutdown a year are expected. Depending upon the duration of shutdown and the number of preceding shutdowns the effectiveness of poison will be reduced for a

subsequent shutdown. The implications of this aspect alongwith partial insertion of shutdown rods needs to be studied.

5.3.2 Number of redundant components required can be reduced if frequent testing and maintenance is undertaken. This, however, affects the system performance and increases unavailability. An optimisation problem can be formulated to minimise the cost of providing redundant components, testing and maintenance procedures and the cost of reduced output of reactor system as a function of n, frequency of testing and maintenance and the duration of testing and maintenance procedures.

5.3.3 A 'failure' can be either a 'Safe failure' or an 'unsafe failure' depending upon the consequences. Inadvertant trip of a reactor is a 'safe failure' from the point of view of reactor safety but is certainly a nuisance from reactor operations consideration. It is desirable that spurious reactor trip should not occur and an analysis of this will be needed to determine reactor power system availability.

Table 5.1: Unavailability per demand of Reactor Protection System.

Basic Assumptions: 1. Constant Failure-rate

2. Fault Exposure Time : 720 hrs. (1 month)

3. One demand during fault exposure duration (for present study only)

Source	Reactor Type	Protection System	Unavailability per demand			Remark
			Lower limit	Upper limit	Best location estimate	
WASH-1400 [32]+	PWR	SCRAM ROD (EMSR)	2.35×10^{-3}	4.58×10^{-2}	3.25×10^{-3}	Failure to insert single rod+testing and maintenance unavailability
WASH-1400 [5]	PWR	SCRAM SYSTEM	1.3×10^{-5}	1.0×10^{-4}	3.6×10^{-5}	Out of total 48 rods, 2 redundant
ULLRICH et.al [21]	PWR	SCRAM SYSTEM			10^{-5}	
PRESENT STUDY	CANDU	SCRAM ROD (EMSR)	1.524×10^{-2}	1.346×10^{-1}	4.55×10^{-2}	System mechanics considered
	CANDU	SCRAM SYSTEM	1.137×10^{-3}	0.289	2.39×10^{-2}	Out of 14 rods, 2 2 redundant
	CANDU	LPR(Single)	3.67×10^{-2}	2.69×10^{-1}	0.1	System mechanics considered
	CANDU	LPR System			0.0158	12/14 logic
	CANDU	Combined system			3.776×10^{-4}	

+ Only instrumentation analysed. Mechanical system omitted.

Table 5.2: Required Number of Redundant Components

NB: q : component unavailability

m : specified minimum number of components

r : minimum number of redundant components required to give a lower system unavailability compared to component unavailability.

	m = 12		m = 46	
	Range of q	r	Range of q	r
1.	$0.0 \leq q < 0.07$	1	$0.0 \leq q < 0.02$	2
2.	$0.07 \leq q < 0.13$	2	$0.02 \leq q < 0.03$	3
3.	$0.13 \leq q < 0.19$	3	$0.03 \leq q < 0.05$	4
4.	$0.19 \leq q < 0.25$	4	$0.05 \leq q < 0.07$	5
5.	$0.25 \leq q < 0.30$	5	$0.07 \leq q < 0.08$	6
6.	$0.30 \leq q < 0.35$	6	$0.08 \leq q < 0.10$	7
7.	$0.35 \leq q < 0.39$	7	$0.10 \leq q < 0.12$	8
8.	$0.39 \leq q < 0.43$	8	$0.12 \leq q < 0.13$	9
9.	$0.44 \leq q < 0.46$	9	$0.13 \leq q < 0.15$	10
10.	$0.46 \leq q < 0.49$	10	$0.15 \leq q < 0.16$	11
11.	$0.49 \leq q < 0.52$	11	$0.16 \leq q < 0.18$	12
12.	$0.52 \leq q$	12	$0.18 \leq q$	46

REFERENCES

1. WASH-1400: Reactor Safety Study,U.S. Nuclear Regulatory Commission (NRC), 1975, Main Report.

2. Kastenberg, W.E., McKone, T.E. and D. Okrent,'Risk Assessment in the Absence of Complete Data', Nucl. Engg. and Design, 44 (1977), pp. 135-146.

3. Smith, T.H., Pelto, P.J., Stevens, D.L., Seybold,G.D., Purcell, W., and L.V. Kimmel, 'A Risk based fault tree analysis method for identifications - preliminary evaluation and screening of potential accidental release sequences in Nuclear Fuel Cycle Operations', BAWL 1959, UC-70, Jan. 1976.

4. WASH-1400: Reactor Safety Study, U.S.N.R.C., 1975, Appendix 1.

5. WASH-1400: Reactor Safety Study, U.S.N.R.C., 1975, Appendix 2.

6. Rasmussen, N.C., Veseley, W.E., and Mitsurw Malkawa,'An Application of Risk Analysis Functional Relationships of Nuclear Risks', Ref.9.

7. Veseley, W.E., 'Analysis of Fault Trees by Kinetic Tree Theory', IN-1330, Oct. 1969.

8. Veseley, W.E., 'A Time dependent methodology for Fault Tree Evaluation', Nucl.Engg. and Design, 13(2), August 1970.

9. Fussell, J.B. (Ed.), 'Nuclear System Reliability Engineering and Risk Assessment', SIAM (1977).

10. Fussell, J.B., 'Synthetic Tree Model A Formal Methodology for Fault Tree Construction', ANCR 1098, March, 1973.

11. Lapp and G.J. Powers,' Computer Aided Synthesis of Fault Trees', IEEE Transactions on Reliability, April, 1977.

12. Apostolakis, G.E., and Yum Tong Lee, 'Method for the Estimation of Confidence Bounds for the TOP event Unavailability of Fault-Trees,' Nucl.Engg. and Design, Vol. 41, 1977.

13. Salem, S.L., Apostolakis,G.E., and D. Okerent,'A New Methodology for the Computer-Aided Construction of Fault Trees', Annals of Nuclear Energy, Vol.4(1977).

14. Taylor, J.R., 'A Formalisation of Failure Mode Analysis of Control Systems', Danish Atomic Energy Commission, RISO-M-1654.

15. Fussel, J.B. and W.E.Veseley, 'A New Methodology for Obtaining Cut-Sets for Fault Trees', ANS Transactions, Vol. 15, June 1972.

16. Somanderes, S.N., 'ELRAFT - A Computer Program for Efficient Logic Reduction Analysis of Fault Trees', IEEE Transactions on Reliability, Nov. 1970.

17. Schneewis,W.G., 'Calculating the Probability of Boolean Expression Being 1', IEEE Transaction on Reliability, Vol. R-26, April, 1977.

18. Chamow, Martin F., 'Directed Graph Techniques for the Analysis of Fault Trees', IEEE Trans. on Reliability, Vol. R-27, No. 1, April, 1978.

19. Apostolakis,G.E., and Ali Mosteh, 'A Study on the Quantification of Judgement', Presented at the ANS Meeting on Probabilistic Analysis of Nuclear Reactor Safety, Newport Beach, California, May 8-10, 1978.

20. Fullwood, R.R., Erdmann , R.C., Rumble, E.T., and G.S. Lellouche, 'Application of the Bayes Equations to Predicting Reactor System Reliability', Nuclear Technology,Vol. 34, August 1977.

21. Ullrich, W., and W. Frisch, 'Investigation of Anticipated Transients Without Reactor Scram and Other Related Safety Devices', Nuclear Technology, Vol. 41, Dec. 1978.

22. WASH 1400 : Reactor Safety Study, U.S.N.R.C. 1975, Appendix 3.

23. Y.Chellam, 'A Compendium of Failure Rate Data on Selected Electronic, Electrical and Mechanical Items from Available Sources as Listed', Reliability Evaluation Laboratory, Bhabha Atomic Research Centre, Bombay.

24. Private Communication of Mr. A. Bhoomiah, PPED, DAE, India.

25. Private Communication of Mr. P. Arumugham, BHEL, India.

26. Buckland, W.R., 'Statistical Assessment of Life Characteristics', Griffin Statistical Monograph and Courses (1964).

27. Richard C. Beercheck, 'How dirt and Water Slash Bearing Life', Machine Design, July 6, 1978.

28. Shapiro, A.H., 'The Dynamics and Thermodynamics of Compressible Fluid Flow', Vol. II, 1954, The Ronald Press Company, New York,

29. Shapiro, A.H., 'The Dynamics and Thermodynamics of Compressible Fluid Flow', Vol. I.

30. Apostolakis, G.E., 'The Effect of a Certain Class of Potential Common Mode Failures on the Reliability of Redundant Systems', Nucl. Engg. and Design, Vol.36, No. 1, Jan. 1976.

31. WASH-1400 : Reactor Safety Study, U.S.N.R.C. 1975, Appendix 4.

32. Leverenz, F.L., A.A. Garcia, and J.K. Kelley, 'Probabilistic Analysis of the Interfacing System Loss of Coolant Accidents on Design Decisions', Nuclear Technology, Vol. 37, Jan. 1978.

APPENDIX A

MATHEMATICAL MODEL FOR ELECTROMECHANICAL SHUTDOWN ROD

The model computes time required by shutdown rod to traverse the distance from point of suspension down to the support in guide tube against the forces due to friction between various components, damping due to moderator i.e. buoyancy and viscous drag and energy imparted to rotating components. The acceleration of rod at any given time t after the release of magnetic clutch is given by the ratio of apparent weight to real weight times the acceleration due to gravity, hence,

$$a(t) = \frac{W+wL_o-B_o + Wl(t) - B(t) - F(t) - \sum \frac{I\theta^o}{v} \frac{d\theta^o}{dt}}{W + wL_o + wl(t)} g \qquad (A.1)$$

In this expression,

$l(t) = \int_o^t dt \int_o^t dt\, a(t)$; length of rope at time t, c

$W+wL_o - B_o$ = apparent weight of suspended system at time t = 0

B_o = Buoyancy (at t = 0) = $\rho_w \pi R^2 g H_o$ (A.2)

$B(t)$ = Buoyancy plus viscous drag at any time t minus B_o

$= \rho_w \pi R^2 g l(t) + f \frac{\pi R^2}{D_e} \frac{\rho_w}{2} l(t) v^2(t)$ (A.

where $v(t) = \int_o^t a(t)\, dt$, velocity of rod at time t, cm/sec

A.1 Computation of Frictional forces, F(t):

Sum of all frictional forces is given by,

$$F(t) = F_{P1}(t) + F_{P2}(t) + F_D(t) + F_{G12} + F_{G23}$$

A.1.1 Calculation of $F_{P2}(t)$:

Fig. A.1 shows the forces acting on the pulley P2.

Resolving the forces into vertical and horizontal components,

$$\text{downward component} = T_1 + F_{P1} + W_{P2} - T_2S_2$$

$$\text{Horizontal component} = T_2C_2$$

Pressure on the bearings P_2 is given by,

$$P_2^2 = (T_1 + F_{P2} + W_{P2} - T_2S_2)^2 + (T_2C_2)^2 \qquad (A.4)$$

if, μ_B is frictional coefficient in bearings then

$$F_{P2}^2 = \mu_B^2 P_2^2 \qquad (A.5)$$

From eqns.(A.4)and(A.5),

$$F_{P2}^2 = \mu_B^2 [(T_1 + F_{P2} + W_{P2} - T_2S_2)^2 + (T_2C_2)^2] \qquad (A.6)$$

where, T_1+F_{P2} = downward tension in rope

$$= W + wL_o - B_o + wl(t) - B(t) = T(t) \qquad (A.7)$$

$$T_2 = T_1E_2$$

$$= [T(t) - F_{P2}] E_2$$

F_{P2} is considerably small compared to T(t), hence

$$T_2 \simeq T(t) E_2 \qquad (A.8)$$

Substituting (A.7) and (A.8) into (A.6) gives

$$F_{P2} = \mu_B \left[(1-E_2S_2)T(t) + W_{P2} \right]^2 + E_2C_2T(t)^2 \Big]^{\frac{1}{2}} \quad (A.9)$$

A.1.2 Calculation of F_{P1}

Fig. A.2 shows forces acting on pully P1. The rope is not assumed to be weightless. Then

$$T_2'(t) + F_{P1} = T_2(t) + wL_{12}C_2 = T_o(t) \quad (A.10)$$

$$T_3 = (T_o - F_{P1})\, E_1 \quad (A.11)$$

Then pressure on bearing P_2 is given by

$$P_1^2 = (T_3S_1 + T_oS_1)^2 + (T_oC_1 - T_3C_1 + W_{P1})^2$$

Since $F_{P1} \ll T_o$, $T_3 \simeq T_oE_1$

hence

$$F_{P1} = \mu_B \left[(1+E_1)^2 S_1^2 T_o^2 + ((1-E_1)\, C_1\, T_o + W_{P1})^2 \right]^{\frac{1}{2}} \quad (A.12)$$

A.1.3 Calculation of $F_D(t)$

Figure A.3 shows forces acting on the drum. Since rope is not weightless,

$$T_3' + F_D = T_3 + wL_{D1}\, C_3 \quad T_{01}(t) \quad (A.13)$$

Thrust acting on bearing P_D is given by,

$$P_D^2 = (T_{01}C_3 + W_D)^2 + T_{01}^2 S_3^2$$

Hence,

$$F_D = \mu_B \left[(T_{01}\, C_3 + W_D)^2 + T_{01}^2\, S_3^2 \right]^{\frac{1}{2}} \quad (A.14)$$

A.1.4 Contribution to F (t) by Gears G1, G2 and G3:

The friction due to shaft bearing gears and bearing for G1 and G2 is negligible. It is therefore sufficient to consider friction between gear teeth. To compute this term sliding friction (coefficient of friction μ_s) between the teeth of two gears is considered. At any given moment on average 2 pairs of surfaces are sliding against each other.

Torque due to tension T_3' about the axis of drum $= T_3'(t)\ R_D$,

neglecting the torque lost in bearings due to friction, the force acting on the gear teeth is approximately given by

$$F_{T32} = \frac{T_3'(t)\ R_D}{R_{G3}} \qquad (A.15)$$

Hence friction due to Gears G2 and G3,

$$F_{G32} = 2\mu_s\ F_{T32} \qquad (A.16)$$

Because G2 and G1 are of same size and once again neglecting loss of torque due to friction,

$$F_{G21} = 2\mu_s\ F_{T32} \qquad (A.17)$$

A.2 Computation of Deceleration due to Moment of Inertia of Rotating Components:

The inertial effect of all rotating components other than drum on the acceleration of shutdown rod is negligible because of very low moment of inertia. The problem is now that of an apparent mass m suspended by a rope wound over a drum of mass M. The initial acceleration of mass is a_o. It can be shown that because of the inertia of drum the modified acceleration a is given by,

$$a = \frac{m \frac{D^2}{4}}{I_{drum} + m \frac{D^2}{4}} a_o \qquad \text{(A.18)}$$

where D : diameter of drum

I_{drum}: moment of inertia of drum $= \frac{1}{2} \cdot M \frac{D^2}{4}$

The apparent mass of rod is given by

$$m(t) = \frac{W(t) + wl(t)\, B(t) - F(t)}{a_o} \qquad \text{(A.19)}$$

Notations:

$a(t)$	:	acceleration of rod at time t, cm/sec.^{2}
f	:	Darcy's friction coefficient
g	:	acceleration due to gravity, cm/sec.^{2}
w	:	weight of rope, Kgf/cm.
C_1	=	Cos θ_1, C_2 = Cos θ_2, C_3 = Cos θ_3
D_e	:	equivalent diameter of rod, cm
D_i	:	diameter of component i, cm
E_i	:	exp $(-\mu\theta_i)$,
F_i	:	frictional force due to component i
Gij	:	gear ij,
H_o	:	initial length of rod in water
I_i	:	moment of inertia of component i, Kg cm^2
L_o	:	initial length of unwound rope
P_i	:	pulley i
R	:	radius of rod, cm
R_i	:	radius of component i
S_i	:	Sin θ_i,
T	:	tension in rope, Kgf.
W	:	weight of rod, Kgf.
ρ_w	:	density of water
μ_B	:	coefficient of friction in bearing
μ_S	:	sliding coefficient of friction

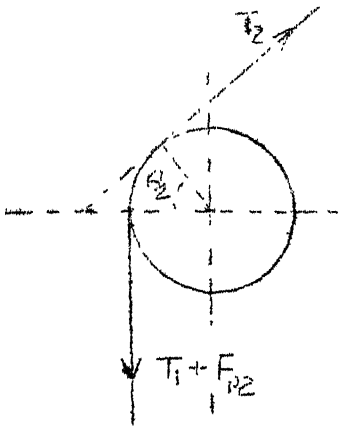


FIG A.1 PULLEY P2

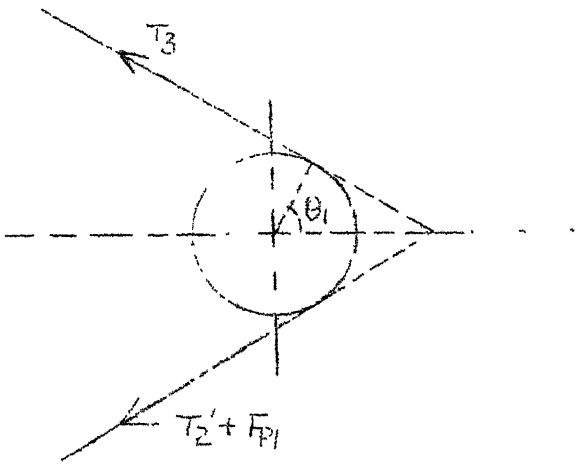


FIG.A.2 PULLEY P1

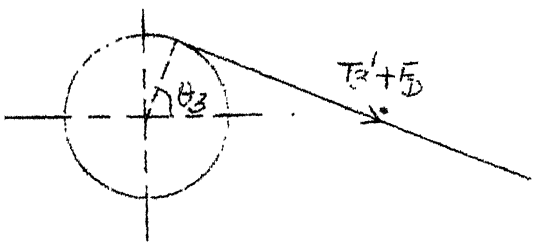


FIG. A.3 DRUM

APPENDIX B

MATHEMATICAL MODEL FOR LIQUID POISON ROD SHUT-OFF

The model computes the time required to fill a liquid poison rod after receiving the scram signal. As was described in Chapter 2, the liquid injection into the rod takes place because of the equalisation of pressures in the two tanks (LHT and GHT) triggered by the scram signal. Because the He-gas pressure in the two tanks and the liquid head in the piping is continuously changing the liquid flow is essentially unsteady, so will be the flow of gas from one tank to another, and the problem therefore involves interaction of gas flow circuit and liquid flow circuit. One should also include the time characteristics of the opening of valve. We have, however, assumed that after receiving scram signal 100 % opening of valve is available in order to avoid complications of dynamics of fluid flow because of changing aperture of valve. To include the time delay effect a correction time is applied to the time required to fill the liquid poison rod.

B.1 LIQUID FLOW CIRCUIT:

Fig. B.1 shows the liquid flow circuit of the system at some time t. Thermodynamical property changes of liquid poison are neglected. The control volume at time t as shown

by dotted lines and we now apply basic laws of continuous media to this control volume.

CONTINUITY EQUATION:

The integral form of continuity equation is,

$$\oint_{c.s.} \rho \vec{V}. \vec{dA} = -\frac{\partial}{\partial t} \int_{v} \rho \, dv \qquad (B.1)$$

Because liquid poison is incompressible, ρ = constant

hence $V_1 A_1 = V_2 A_2$ (B.2)

Momentum Equation:

For a control volume fixed in space, the momentum equation is,

$$\vec{F}_B + \vec{F}_S = \oint_{c.s.} \vec{V} (\rho \vec{V}. \vec{dA}) + \frac{\partial}{\partial t} \int_{c.v.} \vec{V} (\rho dv) \qquad (B.3)$$

where $\vec{F}_B$ = Force distribution acting on the material inside the system the system (body force)

$\vec{F}_S$ = Surface forces (force distribution acting on the boundary of system).

For simplicity, shear stresses are neglected.

In applying equation B.3 to liquid flow circuit the convention is that the forces acting in the direction of flow are positive. With reference to Fig. B.1,

$$F_B = \rho_1 \, g \, [A_1 \ell_1 + A_2(\ell_2 + \ell_3 - \ell_4)] \qquad (B.4)$$

F_S = Reaction force acting on fluid in tank 1 + Friction force + Forces acting on the end surfaces of liquid.

$$= -[P_1 + \rho_\ell g \ell_1](A_1 - A_2) - \frac{f V_2^2 A_2}{2 \rho_\ell} \left(\frac{A_2}{A_1} \frac{\ell_1}{D_1} + \frac{\ell_2}{D_2} + \frac{\ell_3}{D_2} + \frac{\ell_4}{D_2} \right) + P_1 A_1 - P_2 A_2 \qquad (B.5)$$

On algebraic manipulations,

$$F_B + F_S = A_2 \rho_2 g [\ell_1 + \ell_2 - \ell_4] + (P_1 - P_2) A_2 - \frac{f V_2^2 A_2}{2 \rho_\ell} \left[\frac{A_2}{A_1} \frac{\ell_1}{D_1} + \frac{\ell_2 + \ell_3 + \ell_4}{D_2} \right] \qquad (B.6)$$

Term,

$$\left| \oint_{c.s.} \vec{V} (\rho \vec{V} . \vec{dA}) \right| = - \rho_\ell V_1^2 A_1 + \rho_\ell V_2^2 A_2 = \rho_\ell A_2 V_2^2 \left(1 - \frac{A_2}{A_1}\right) \qquad (B.7)$$

$$\left| \int_V \vec{V} \rho_\ell dv \right| = \int_{V_1} \vec{V} \rho_\ell A_1 dl_1 + \int_{V_2} \vec{V} \rho_\ell A_2 \, dl_2 + \int_{V_3} \vec{V} \rho_\ell A_3 \, dl_3 + \int_{V_4} \vec{V} \rho_\ell A_4 \, dl_4 \Big|$$

$$= V_1 \rho_\ell A_1 \ell_1 + V_2 A_2 \rho_\ell (l_2 + l_3 + l_4)$$

$$= V_2 \rho_\ell A_2 \left[\frac{A_1}{A_2} l_1 + l_2 + l_3 + l_4 \right]$$

hence,

$$\left| \frac{\partial}{\partial t} \int_V \vec{v} \rho \, dv \right| = \rho_\ell \, A_2 \left(\frac{A_1}{A_2} l_1 + l_2 + l_3 + l_4 \right) \frac{dV_2}{dt}$$

$$+ \quad A_2 \, V_2 \left(\frac{A_1}{A_2} \frac{dl_1}{dt} + \frac{dl_4}{dt} \right)$$

$$= \quad \rho_\ell A_2 \left(\frac{A_1}{A_2} l_1 + l_2 + l_3 + l_4 \right) \frac{dV_2}{dt}$$

$$+ 2 \rho_\ell A_2 \, V_2^2 \qquad \text{(B.8)}$$

Equating eqns. (B.6) and (B.8) + (B.7), and on simplification,

$$C_1(t) \frac{dV_2}{dt} + C_2(t) \, V_2^2 - C_3(t) = P_1(t) - P_2(t) \qquad \text{(B.9)}$$

where,

$$C_1(t) = \rho_\ell \left(\frac{A_1}{A_2} l_1 + l_2 + l_3 + l_4 \right) \qquad \text{(B.10)}$$

$$C_2(t) = \rho_\ell \left(1 - \frac{A_2}{A_1}\right) + 2 \rho_\ell + \frac{f}{2} \rho_\ell \left(\frac{A_2}{A_1} \frac{l_1}{D_1} + \frac{l_2 + l_3 + l_4}{D_2} \right) \qquad \text{(B.11)}$$

$$C_3(t) = + \rho_\ell \, g \, (l_1 + l_2 - l_4) \qquad \text{(B.12)}$$

B.2 GAS FLOW CIRCUIT:

The problem of gas flow circuit needs to be solved to produces functions $P_1(t)$ and $P_2(t)$. The basic problem is find gas flow from a high pressure tank H to a low pressure tank L. The fluid is compressible and because of changing pressure the flow is unsteady, there is friction due to interconnecting pipe and thermodynamic property changes will

take place. Another element of complication is due to the fact that gas flow will be near mach number of 1.

An exact formulation of the problem is possible [28] but because of the computational complexity the unsteady flow is assumed to be steady over a small time interval. In case of small interconnecting pipes the gas flow can be assumed adiabatic [29]. Therefore, the problem is now of solving a steady, adiabatic gas flow through constant area duct with friction. This is a standard problem whose solution is available in advanced texts [29]. Below we give relevant results.

Fig. B.2 illustrates the physical situation. The equation relating the two pressures P_H and P_L is,

$$\frac{P_H}{P_L} = \frac{M_L}{M_H} \sqrt{\frac{1 + \frac{K-1}{2} M_H^2}{1 + \frac{K-1}{2} M_L^2}} \qquad \text{(B.13)}$$

M_H and M_L are velocities of gas at the two ends in mach numbers. From this equation given P_H, P_L and M_H, M_L can be found. By using mass balance and gas law pressure changes in H and L can be computed. M_H can be obtained by assuming isentropic pressure change in high pressure cylinder. This can be done by using [29],

$$M_H = \left\{ \frac{2}{K-1} \left[\left(\frac{p_o}{p} \right)^{\frac{K-1}{K}} - 1 \right] \right\}^{\frac{1}{2}} \qquad \text{(B.14)}$$

where p is the present pressure and p_o is stagnation pressure (pressure corresponding to $M_0 = 0$), in our case initial pressure.

We now extend these relation to the LPR shutoff system.

B.2.1 BOOSTER CYLINDER:

The exit velocity of gas from booster cylinder is given by using eqn. B.14,

$$M_B = \left\{ \frac{2}{K-1} \left[\left(\frac{P_{oB}}{P_B} \right)^{\frac{K-1}{K}} - 1 \right] \right\}^{\frac{1}{2}} \qquad (B.15)$$

Hence, $v_B = CM_B = M_B \sqrt{\frac{KP_B}{\rho_B}}$.

Assuming steady state condition for small time interval t,

gas outflow rate $= \rho_B A v_B$

where A is cross-sectional area of interconnecting pipe.

Also, Gas outflow rate $= -\frac{d}{dt}(V_B \rho_B) = -\frac{V_B}{R_B}\frac{dP_3}{dt}$

where,

$R_B = \frac{P_B}{\rho_B} = \frac{Po_B}{\rho_{oB}} \frac{T_B}{T_{oB}}$ and it constant over time interval t. Therefore, equating two gas flow rates,

$$\frac{dP_B}{dt} = -\frac{P_3 A v_B}{V_B} \qquad (B.16)$$

Since, PV = m RT (Ideal Gas Law)

$$\frac{dT}{dt} = T \left[\frac{1}{P} \frac{dP}{dt} - \frac{1}{m} \frac{dm}{dt} \right]$$

hence,

$$\frac{dT_B}{dt} = T_B \left[\frac{1}{P_B} \frac{dP_B}{dt} - \frac{1}{m_B} \frac{dm_B}{dt} \right] \qquad (B.17)$$

where,

$$m_B = \rho_B V_B$$

B.2.2 Gas Header Tank:

Gas exit velocity is given by,

$$M_G = \frac{2}{K-1} \left[\left(\frac{P_{oG}}{P_G} \right)^{\frac{K-1}{K}} - 1 \right]^{\frac{1}{2}} \qquad (B.18)$$

Hence $v_G = M_G \sqrt{K \frac{P_G}{\rho_G}}$

Assuming steady state conditions prevail,

$$\text{gas outflow rate} = \rho_G A v_G$$

$$\text{also, gas outflow rate} = - \frac{d(V_G \rho_G)}{dt} = - \left[V_G \frac{d\rho_G}{dt} + \rho_G \frac{dV_G}{dt} \right]$$

$$= - \frac{V_G}{R_G} \frac{dP_G}{dt} - \rho_G A_2 V_2$$

Equating the two gas outflow rates,

$$\frac{dP_G}{dt} = - \frac{R_G}{V_G} \left[\rho_G A v_G - \rho_G A_2 V_2 \right] \qquad (B.19)$$

and it can be shown that,

$$\frac{dT_G}{dt} = T_G \left[\frac{1}{P_G} \frac{dP_G}{dt} - \frac{A_2 V_2}{V_G} + \frac{1}{m_G} \frac{dm_G}{dt} \right] \qquad (B.20)$$

where m_G = mass of gas in GHT and LPR.

B.2.3 Liquid Header Tank:

Gas enters LHT from two sources viz. GHT and Booster cylinder. Velocity of Gas received from Booster cylinder is obtained by solving eqn. (B.13),

$$M_{LB} = \left[\left(\frac{P_B}{P_L}\right)^2 \frac{M_B^2}{1 + \frac{K-1}{2} M_B^2} - \frac{K-1}{2} \right]^{-\frac{1}{2}} \qquad (B.21)$$

Similarly, velocity of Gas received from GHT is given by,

$$M_{LG} = \left[\left(\frac{P_G}{P_L}\right)^2 \frac{M_G^2}{1 + \frac{K-1}{2} M_G^2} - \frac{K-1}{2} \right]^{-\frac{1}{2}} \qquad (B.22)$$

corresponding velocities are, $v_{LB} = M_{LB} \sqrt{K \frac{P_L}{\rho_L}}$,

and $v_{LG} = M_{LG} \sqrt{K \frac{P_L}{\rho_L}}$

Gas inflow rate $= \frac{d}{dt} (\rho_L V_L) = \rho_L A_1 (v_{LB} + v_{LG})$

or, $\rho_L \frac{dV_L}{dt} + \frac{V_L}{R_L} \frac{dP_L}{dt} = \rho_L A_1 (v_{LB} + v_{LG})$

hence,

$$\frac{dP_L}{dt} = \frac{P_L}{V_L} [A_1 (v_{LB} + v_{LG}) - A_1 V_1] \qquad (B.23)$$

and it can be shown that,

$$\frac{d\,T_L}{dt} = T_L \left[\frac{1}{P_L} \frac{dP_L}{dt} + \frac{A_1 V_1}{V_L} - \frac{1}{m_L} \frac{dm_L}{dt} \right] \qquad (B.24)$$

The computer program LPSHUT executes the above formulation.

Notations:

A_i : area of cross-section at section i

D_i : diameter of pipe at section i

M_i : Mach number at section i

P : He-gas pressure

V_i : velocity of fluid at section i

g : acceleration due to gravity

l_i : length of pipe i

ρ_l : density of liquid poison

ρ_i : density of He gas in tank i; i = B,L or G.

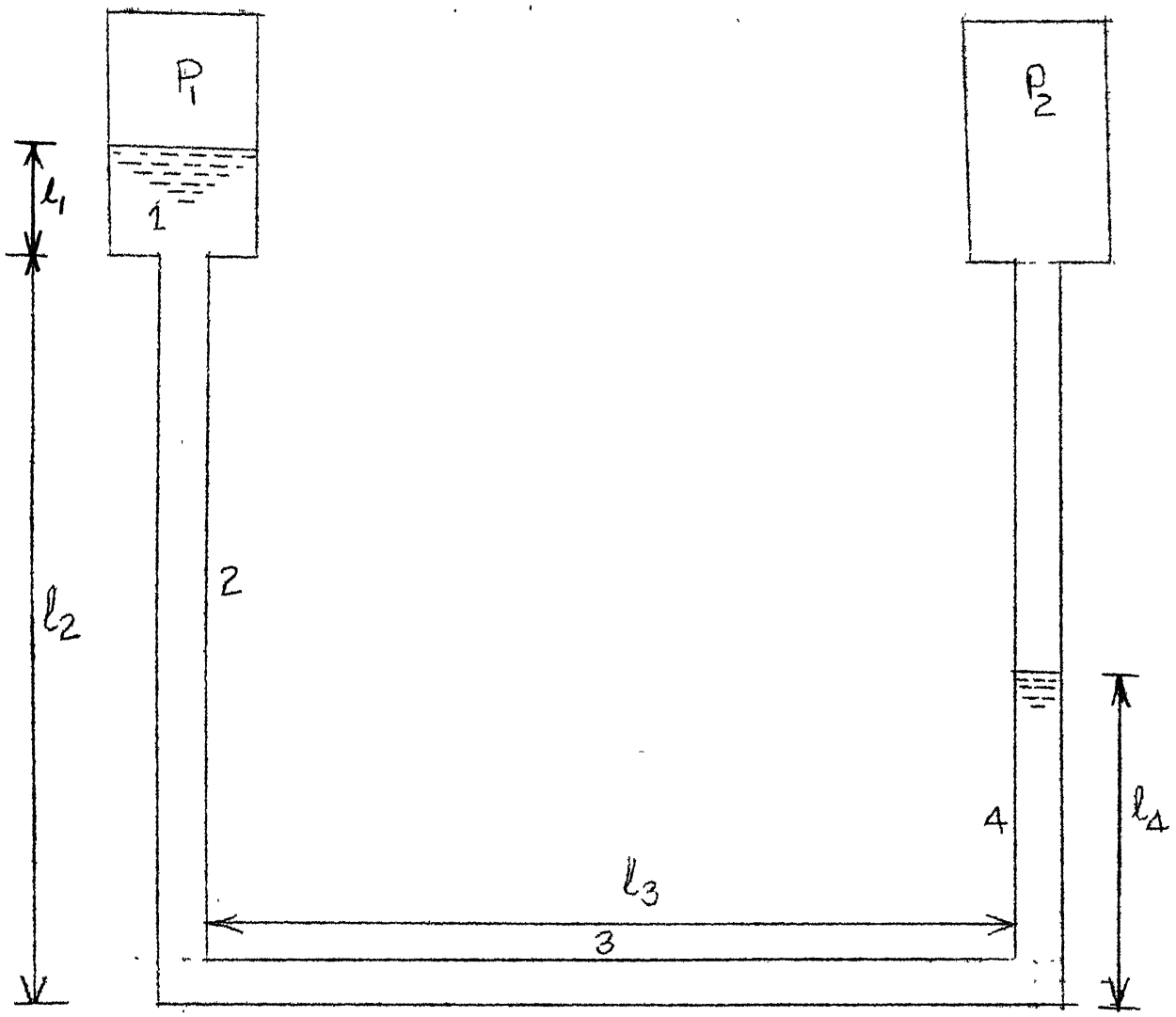


FIG. B.1 LIQUID FLOW CIRCUIT

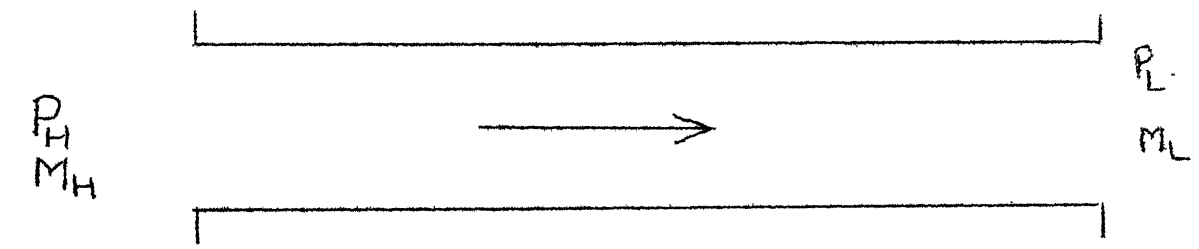


FIG. B.2: GAS FLOW

APPENDIX C

DATA TREATMENT AND UNAVAILABILITY ESTIMATION

C.1 DATA TREATMENT:

It has been emphasized before that failure data on reactor systems is either not available or is highly sparse, same holds true for the data on basic component failure. Therefore,it becomes inevitable to collect failure data on basic components from other industries. Since components designed to perform similar function in different industries may have different designs, are manufactured by different companies and are exposed to different environment in application, it is natural to expect that failure data thus collected will exhibit large scatter. In such a situation it is not possible to assign a point estimate of failure rate for generic components and failure rate has to be treated as a random variable and a probability density function is assigned to this random variable.

The treatment of data as random variables serves as a means to describe the uncertainity of the data. The range of random variable gives possible values that the random variable can take and probability distribution assigned gives the likelihood that the data value will actually be any one of the given values in this range.

For the present study failure data was obtained from WASH-1400 [22] and reference [23]. Reference [23] gives mean, upper bound and lower bound on the failure rate and it can be assumed that sufficient field data was available to allow such estimates. WASH-1400 reports 5 percentile and 95 percentile values of the field data and assessed median value by fitting lognormal distribution to the available data. The reasons put forward in support of lognormal distribution by the report can be summarized as:

'Lognormal is a natural distribution for describing data which can vary by factors, it has an adequate shape to represent field data, it is flexible, it is consistent with reliability and data properties and it is standardly employed distribution'.

It may be noted that the shape of distribution corresponding to lognormal i.e. a peak and skewness towards right, and the 5 and 95 percentile values can be treated as emperical information. Furthermore, because of large variance in data (it is almost equal to median value) it is not very meaningful to strive for an accurate location parameter estimate. It should instead be preferable to obtain a distribution giving lower variance than lognormal and based on same emperical information. Other distributions mentioned in literature are Gamma and Weibull [6]. Gamma has been used in bayesian estimation of reliability because it is conjugate to Poisson distribution and gives closed form posterior. Weibull, on the

other hand, has the advantages of being more flexible and having a closed form distribution function. Therefore, Weibull distribution was tried on data from WASH-1400 and ref. [19] and the one having proper shape and lower variance among Weibull and Lognormal were chosen. Results are tabulated in Table C.2.

C.2 UNAVAILABILITY ESTIMATION [5]:

Unavailability is the probability that a system when used under stated conditions shall not operate satisfactorily over a given time interval. TOP event of a fault-tree defines the condition for unsatisfactory operation of the system in terms of hardware performance. The probability of TOP event, therefore, gives unavailability of the system. TOP event can be expressed as a Boolean algebra function of primary events. This function should be logically simplified to eliminate redundant events and to do so following basic properties and laws of Boolean algebra are used.

a. Identities:

1. $A + A = A$
2. $A \cdot A = A$

b. Distributive Laws:

1. $A(B+C) = (A.B) + (A.C)$
2. $A+(B.C) = (A+B) \cdot (A+C)$

C. Laws of Absorption:

1. $A + (A.B) = A$

2. $A \cdot (A.B) = A.B$

In case of complex fault trees mere algebraic simplification becomes tedious and one can use decision table method or Karnaugh graph method. The essential idea is to obtain all the minimal cut sets of the TOP event such that we can write, after simplification, TOP event as

$$T = M_1 + M_2 + \ldots + M_n \qquad (C.1)$$

where M_i, the minimal cut-set, is intersection of primary events C_{ik},

$$M_i = C_{i1}\, C_{i2}\, C_{i3} \cdots C_{im} \qquad (C.2)$$

and no M_i is a subset of another M_j. The minimal cutsets, also termed critical paths are important because they specify a unique,failure mode' by which the TOP event can occur. Decomposition of TOP event into all possible critical paths is not essential if we are only interèsted in the TOP event failure probability. However, identification of all possible critical paths becomes inevitable if Risk estimation is to be done where each failure mode will have different consequence.

Once the TOP event is expressed as a simplified boolean function of primary events, the probability of the former can be related to that of later by use of basic operational laws to combine probability and given below:

a. UNION:

Boolean Expression: $T = A+B$

Probability expression:

$$P(T) = P(A) + P(B) - P(A.B)$$

b. INTERSECTION:

Boolean expression: $T = A.B$

Probability expression:

$$P(T) = P(A).P(B/A), \quad \text{if A and B are dependent}$$

or $P(T) = P(A).P(B)$, if A and B are independent

The rare event approximation is applicable when the intersection probability P(A.B) is much smaller than the individual probabilities, P(A) and P(B). If A and B are independent then P(A.B) = P(A).P(B), and the rare event approximation will be valid if cross product term P(A).P(B) is much smaller than P(A) and P(B). This will be the case when P(A) and P(B) are less than approximately 0.1 [5]. Whether the events are independent or dependent and regardless of the probabilities, the rare event approximation will always give a conservative estimate. The approximation in general is also quite accurate [5].

Applying probability laws given above to TOP event expression of eqn. (C.1) we get

$$P(T) = \sum_{i=1}^{n} P(M_i) - \sum_{\substack{j=1 \\ (i \neq j)}}^{n} \sum_{i=1}^{n} P(M_i)P(M_j)$$

+ Probability of all possible triple combinations

If rare event approximation is applied then

$$P(T) \simeq \sum_{i=1}^{n} P(M_i) \qquad (C.3)$$

If primary events are independent,

$$P(M_i) = \sum_{k=1}^{m} P(C_{ik}) \qquad (C.4)$$

C.3 UNAVAILABILITY CONTRIBUTIONS [4]:

Component unavailability is defined as the probability of being in a failed state when required. The particular contributions to component unavailability that arise in analyses are broken as below:

C.3.1 FAILURE UPON DEMAND:

It comprises of failure of a component to start e.g., a pump failing to starts, and failure of demand itself e.g., failure of a control signal to be transmitted to the component. The demand can be automatically initiated or manually initiated by the operator. In the later case it is failure of operator, i.e., a human error of omission. The failure upon demand contributions Q are directly given by the demand data in the data base

$$Q = Q_d$$

where Q_d is unavailability per demand.

C.3.2 UNREPAIRED FAILURE CONTRIBUTIONS:

The unavailability contribution for unrepaired failures is given by,

$$Q = \lambda\tau$$

where λ is the failure rate and τ the average fault duration time for which the failure can exist after detection. If component is not monitored but periodically tested then τ is one-half of the test interval.

C.3.3 TEST OUTAGES:

If the component is disabled in on-line periodic testing then the unavailability contribution is,

$$Q = \frac{t_D}{t_T}$$

where, t_D is the average test downtime

and t_T is the average interval between tests.

If component is not disabled during testing or there is an override backup then Q is negligible.

WASH-1400 recommends: t_T = 1 month

t_D = 0.72 hr.,

(a lognormal average of 75 min minimum and a 2 hr. maximum.)

C.3.4 MAINTENANCE OUTAGES:

Scheduled maintenance outages contribute to unavailability in a way similar to test outages. For unscheduled maintenance i.e. done when required, the unavailability is given by,

$$Q = \frac{t_D}{\bar{t}}$$

where $\bar{t}$ is the average time of the maintenance distribution. Above formula can be rewritten as,

$$Q = f \cdot \frac{t_D}{720 \text{ (hrs/mo.)}}$$

where t_D is downtime in hrs, and

$$f = \frac{1}{\bar{t}} \quad (\text{months}^{-1})$$

where $\bar{t}$ is average time in months between maintenance act.

WASH-1400 in general used ;

f = 0.22, which corresponds to a 4.5 months average frequency interval (associated with 90 percent range of 1 month and 12 months).

t_D = 7 hrs. (associated with a range of 0.5 hrs. to 24 hrs. maximum)

The range in downtimes incorporates maintenance error and inefficiency contributions.

C.3.5 TOTAL UNAVAILABILITY:

The total unavailability of the system will be the sum of unavailability contributions discussed above. In general unavailability has the form

$$Q = \frac{MDT}{MDT + MTBM}$$

where MDT : mean down time

MTBM: mean time between maintenance

Fig. C.3 illustrates a typical duty cycle.

If λ is operational failure rate

λ_r is repair failure rate

then $MDT = \frac{1}{\lambda_r}$

$MTBM = \frac{1}{\lambda}$ for unscheduled maintenance

hence,

$$Q = \frac{\lambda}{\lambda + \lambda_r} = \lambda_{eq} \cdot MDT$$

hence,

$$\lambda_{eq} = \frac{\lambda \lambda_r}{\lambda + \lambda_r}$$

If $\lambda \ll \lambda_r$, as is the case with nuclear components $\lambda_{eq} = \lambda$., the operational failure rate and no improvement is expected from unscheduled maintenance, obviously because of low operational failure rate the frequency of unscheduled maintenance will be low.

C.4 CUMULATIVE FAILURE PROBABILITY:

The cumulative failure probability or simply failure probability, is the probability that the component will not operate successfully for a required time period t. The component is supposed to have started successfully and the failure probability refers to operational mode.

For a single component, the failure probability is given by,

$$P = 1 - e^{-\lambda t} \simeq \lambda t$$

where the approximation $P \simeq \lambda t$ is used since it is valid to several significant figures for probabilities less than 0.1.

For n repairable components, in parallel, each having an unavailability of Q_i and operational failure rate λ_i, the failure probability is given by

$$P = \sum_{i=1}^{n} \lambda_i t \left(\sum_{\substack{j=1 \\ j \neq i}}^{n} Q_j \right)$$

For more complicated cases basic laws of probability can be extended [12, 5].

C.5 COMMON MODE FAILURE AND QUANTIFICATION TECHNIQUE:

Common mode failure (cmf) are defined as multiple failures which occur because of a single initiating or

influencing cause. Instead of triggering simultaneous failures, which is the extreme case, the common cause may produce a less severe, but common, degradation of the components. In such a case components may not fail simultaneously but their joint probability of failure can be greatly increased [31]. In brief, any common property of the components introduces dependencies that will lead to cmfs[30]. The common causes can be classified into following [31]:

A. Design defects

B. Fabrication, Manufacturing and Quality Control variations

C. Test, maintenance, and repair errors

D. Human errors

E. Environmental variations (contamination, Temperature, etc.)

F. Failure or degradation due to an initiating failure

G. External Initiations of failure

The contribution of common mode failure can be quantified as a cmf failure rate λ_{cm}. In most of the practical cases λ_{cm} is smaller than the chance failure of a component and can be neglected. However, for a redundant system λ is greatly reduced but λ_{cm} remain constant and becomes significant. Greater the redundancy more dominant is the effect of cmf. Apostolakis [30] has shown that for the case where λ_{cm} is smaller than system chance failure rate, there

exists an initial period T for which cmf dominates. The higher the degree of redundancy greater is the time T, and cmf dominates chance failure by order of magnitude. For the case of redundant components being inspected every T_i and T_i T, the effort should be directed towards decreasing the potential of a cmf, since it is the dominant cause of failure. Conversely, for a given T_i there is a maximum degree of redundancy which is effective in reducing the probability of chance failures and further addition of redundant elements is unnecessary because chance failures are no more important. Before a consideration of cmf is included it has to be ascertained whether the contribution of cmf is really meaningful. Apostdakis [30] has suggested following upper bounds below which cmf contribution can be treated negligible.

Table C.1: Upper bound to λ_{cm} for m-out of n systems (n repairmen)

LOGIC m/n	$\mu = 0$	$\mu > \lambda$
1/2	$(6/7)\lambda$	$2\lambda^2/\mu$
1/3	$(66/85)\lambda$	$3\lambda^3/\mu^3$
2/3	$(30/19)\lambda$	$6\lambda^2/\mu$
1/4	$(60/83)\lambda$	$4\lambda^4/\mu^3$
2/4	$(156/115)\lambda$	$12\lambda^3/\mu^2$
3/4	$(84/37)\lambda$	$12\lambda^2/\mu$

where μ is repair rate.

The problem now addressed is quantification of cmf. It should be observed that in general there will be almost no data to permit realistic treatment of cmf contribution. In such a case it is usual to compute an upper bound through though this has the disadvantage of being highly conservative,

Consider joint failure AB of two failures A and B. Whether A and B are independent or dependent,

$$P(AB) \leq P(A), \quad \text{and } P(AB) \leq P(B)$$

therefore, the best upperbound can be taken as

$$P(AB) \leq \text{Min } [P(A), P(B)]$$

Here, P(AB) can represent both random failure and cmf and the equation therefore gives conservative estimate. If error spread of probabilities is to be incorporated then P(A) and P(B) are replaced by their respective upper bounds.

For a general combination consisting of n failures:

Single Failure Bound:

$$P(A_1 A_2 \ldots A_n) < \text{Min } [P(A_1), P(A_2), \ldots P(A_n)]$$

Double Failure Bound:

$$P(A_1 A_2 \ldots A_n) < \text{MIN } [\text{Probabilities of all double combinations}]$$

Triple Failure Bound:

$P(A_1A_2...A_n)$ MIN [Probabilities of all triple combinations]

:

.

so on.

The various upper bounds are therefore obtained by computing the probabilities of smaller combinations contained in the original, large combination. The upper bounds are obtained not only for minimum, but for any smaller combination probability that is computed.

In determining the range for a cmf probability an upper bound and a lower bound are required to define the range. The upper bound is obtained as has been mentioned above. Lower bound is simply taken as the joint probability of the two events considering them independent. These two ranges, in consistency with the data treatment so far, are treated as 5 and 95 percentile values and an adequate distribution is fitted (Weibull or Lognormal) to obtain lowest variance. The location parameter estimate is chosen as best estimate of cmf probability [4].

Table C.2 Failure Rate Data of Basic Components.

Unit: failures /10^6 hrs.

Component description	Field Data		Weibull Parameters		Lognormal Parameters	
	.05	.95	β	α	m	σ
1. Ball bearing (heavy duty)	0.072	3.53	1.045	1.2349	0.505	1.179
2. Ball bearing (light duty)	0.035	1.72	1.044	0.6	0.244	1.18
3. Welds (Fastners)	10^{-4}	0.1	0.588	0.0156	3×10^{-3}	2.0
4. Elbows, Flanges, Expansion joints	10^{-2}	10.0	0.588	1.56	0.318	2.09
5. Gaskets	0.1	100.0	0.588	15.6	3.176	2.09
6. Gears (general)	0.0118	0.2	1.437	0.132	0.0486	0.86
7. Magnetic clutch	4.1	41.0	1.766	41.0	13.18	0.697
8. Pipe (rupture dia 3")	3×10^{-5}	3×10^{-3}	0.588	3×10^{-3}	9.45×10^{-4}	2.09
9. Pressure gauges	1.35	5.77	2.799	1.544	2.79	0.443
10. Pressure sensors	1.7	7.6	2.72	4.497	3.59	0.453
11. Low Pressure Tank	0.1	0.324	3.46	0.2	0.180	0.356
12. High Pressure Tank	0.044	0.144	3.43	0.089	0.0797	0.36
13. Instrument channels						
a. failure to operate	0.1	10.0	0.883	1.5147	3.893	1.39
b. shift in calibration	3.0	300.0	0.883	45.4	30.0	1.39
14. Springs (heavily stressed)	9.9×10^{-5}	0.1	0.588	0.0156	3.15×10^{-3}	2.096
15. Springs (lightly stressed)	8.9×10^{-2}	0.89	1.766	0.48	0.28	0.698
16. Valves (leak)	7.54×10^{-3}	6.78×10^{-2}	1.851	0.0375	0.0226	0.666
17. Valves (plugged)	2.26	20.34	1.851	11.25	6.78	0.666